EUROPA: AUGE Y CAÍDA DE LAS INVESTIGACIONES PENALES BASADAS EN LA CONSERVACIÓN DE DATOS DE COMUNICACIONES ELECTRÓNICAS

Por

Juan Carlos ORTIZ-PRADILLO

Profesor Titular de Derecho Procesal

Universidad Complutense de Madrid

Instituto de Derecho Europeo e Integración Regional (IDEIR)

juancarlosortiz@ucm.es

Revista General de Derecho Procesal 52 (2020)

RESUMEN

En una Europa fuertemente golpeada por los atentados terroristas cometidos en Madrid y Londres, las autoridades nacionales y europeas se conjuraron para combatir y perseguir eficazmente el terrorismo y el crimen organizado a través de diversas iniciativas legislativas, entre las cuales sobresalía la retención de datos de telecomunicaciones como uno de los instrumentos cruciales para dotar de seguridad a los Estados y facilitar la prevención, investigación y enjuiciamiento del terrorismo y de otras formas de delincuencia grave.

Una década más tarde, este régimen centrado en la conservación preventiva de la información derivada de las comunicaciones digitales con miras a ser utilizada en investigaciones penales y de inteligencia está siendo objeto de demolición por parte del TJUE, debido a la excesiva afectación que supone a los Derechos Fundamentales consagrados en el Derecho de la Unión.

En el presente trabajo se efectúa un análisis de los parámetros interpretativos dispuestos por la jurisprudencia europea, se identifican las fortalezas y debilidades de la legislación española en materia de conservación de datos de comunicaciones electrónicas, y se señala el camino a seguir para cumplir con las directrices europeas y que la reforma interna resulte compatible con el Derecho de la Unión Europea, especialmente en materia de protección del derecho a la vida privada y a la protección de los datos de carácter personal.

PALABRAS CLAVE

Comunicaciones electrónicas, Conservación de datos, Privacidad, Carta Europea de Derechos Fundamentales, Justicia Penal.

SUMARIO

1. EL ESCENARIO. 2. «CRÓNICA DE UNA MUERTE ANUNCIADA»: EL RECHAZO EUROPEO A UNA CONSERVACIÓN SISTEMÁTICA E INDISCRIMINADA DE DATOS. 3. «LOS CUATRO JINETES DEL APOCALIPSIS»: LA DEFINITIVA DEFENESTRACIÓN DE LA LEY ESPAÑOLA SOBRE CONSERVACIÓN DE DATOS RELATIVOS A LAS COMUNICACIONES ELECTRÓNICAS. 3.1. El caballo blanco: la *Victoria* del Ministerio Fiscal en el Asunto C-207/16. 3.2. El caballo rojo: la *Guerra* por delimitar el marco jurídico aplicable a la conservación de datos. 3.3. El caballo negro: el *Hambre* de no poder acudir al mayor granero de información. 3.4. El caballo amarillo bayo: la *Muerte* de las investigaciones basadas en datos conservados de comunicaciones electrónicas. 4. «MUERTE EN VENECIA»: LA APREMIANTE REFORMA DE

LA LEGISLACIÓN ESPAÑOLA. 4.1. La debilidad: la inexistencia de criterios legales objetivos para una «conservación selectiva» de datos. 4.1.1. Criterios subjetivos. 4.1.2. Criterios geográficos. 4.1.3. Criterios materiales o teleológicos. 4.1.4. Criterios temporales. 4.2. La fortaleza: el régimen de la LECrim como canon interpretativo para un «acceso limitado» a los datos. 4.2.1. Requisitos generales. 4.2.2. Requisitos especiales. 4.2.2.1. En función de la tipología o categoría del dato solicitado. 4.2.2.2. En función de la cantidad de datos solicitados o del número de peticiones referidas a un mismo sujeto. 4.2.2.3. En función de la extensión del periodo de tiempo a que se refiera el acceso. 4.2.2.4. En función de la gravedad del delito. 5. BIBLIOGRAFÍA.

EUROPE: THE RISE AND THE FALL OF CRIMINAL INVESTIGATIONS BASED ON THE RETENTION OF ELECTRONIC COMMUNICATIONS DATA

ABSTRACT

After the terrorist attacks in Madrid and London, national and European authorities conjured themselves to combat and prosecute terrorism and organized crime effectively through different legislative initiatives, including the retention of telecommunications data as one of the overriding instruments to provide security for States and facilitate prevention, investigation and prosecution of terrorism and other forms of serious crime.

A decade later, this regime focused on the preventive retention of traffic and location data and other digital information with a view to being used in criminal and intelligence investigations is being demolished by the ECJ, owing to the excessive interference in the fundamental rights set out in EU Law.

This paper analyses the interpretative criteria provided for by ECJ case-law, identifies the strengths and weaknesses of Spanish legislation on the retention of electronic communications data, and points out to the legislator the way forward to comply with European guidelines and to ensure the compatibility of the Spanish legal reform with European Union law, in particular in the area of protection of the right to privacy and the protection of personal data.

KEYWORDS

Electronic comunications, Data retention, Privacy, Charter of Fundamental Rights, Criminal Justice.

SUMMARY

1. THE SCENARIO. 2. «CHRONICLE OF A DEATH FORETOLD»: THE EUROPEAN REJECTION OF SYSTEMATIC AND INDISCRIMINATE DATA RETENTION. 3. «THE FOUR HORSEMEN OF THE APOCALYPSE»: THE DEFENESTRATION OF THE SPANISH LAW ON THE RETENTION OF DATA RELATING TO ELECTRONIC COMMUNICATIONS. 3.1. The white horse: the *Victory* of the Public Prosecutor's Office in Case C-207/16. 3.2. The Red Horse: The *Battle* for delimiting the legal framework to data retention. 3.3. The Black Horse: The *Hunger* of not using the largest Information Barn. 3.4. The Yellow Horse: The *Death* of Investigations Based on Preserved Electronic Communications Data. 4. «DEATH IN VENICE»: THE URGENT REFORM OF SPANISH LAW. 4.1. The Weakness: the lack of objective criteria for a 'selective retention' of data. 4.1.1. Subjective criteria. 4.1.2. Geographical criteria. 4.1.3. Material or teleological criteria. 4.1.4. Temporary criteria. 4.2. The Strength: the Spanish CCP regime as objective criteria for ‘restricted access’ to data. 4.2.1. General Requirements. 4.2.2. Special Requirements. 4.2.2.1. Type or category of the data requested. 4.2.2.2. Amount of data requested or the number of requests relating to the same subject. 4.2.2.3. Duration of the time period to which access relates. 4.2.2.4. Seriousness of the offence. 5. BIBLIOGRAPHY.

1. EL ESCENARIO

La actual Sociedad del siglo XXI es calificada como la «Sociedad de la Información», «Era Digital» o «Era Informática», y se encuentra caracterizada por el trascendental papel que juegan las tecnologías de la información y la comunicación en las actividades humanas. Los avances y descubrimientos científicos en materia tecnológica de las últimas décadas han generado una auténtica revolución —la llamada *cuarta revolución industrial*—, y lo que más nos interesa ahora destacar, ha supuesto un exponencial avance en lo referido a los modos de conservar y comunicar la información. Si lo comparamos con lo que significó la invención de la imprenta a mediados del siglo XV, en términos de capacidad de difundir el conocimiento, los posteriores instrumentos de comunicación —el telégrafo, el teléfono, la radio o la televisión— resultan avances insignificantes si los comparamos con lo que supuso la aparición de Internet, porque precisamente lo que caracteriza nuestro mundo actual es la colosal capacidad de crear, conservar y compartir la información.

En la actual Sociedad Tecnológica, la obtención de cualquier rastro físico o biológico que permita identificar al delincuente y relacionarlo con el hecho punible se ha visto completado —y en muchas ocasiones, sustituido— por la búsqueda de rastros digitales que lo relacionen con la víctima, con los instrumentos o efectos del delito, o con el escenario del crimen. Y en este legítimo objetivo de las autoridades encargadas de una investigación criminal, nos interesa poner de manifiesto las vastas posibilidades que ofrecen las nuevas capacidades de «tecnovigilancia» centradas en la localización, aprehensión y análisis de los datos personales de los ciudadanos para su posterior utilización en el Proceso Penal, las cuales se han visto favorecidas por un nuevo modelo de Economía mundial que Shoshana ZUBOFF ha calificado como «el capitalismo de la vigilancia[1]». Frente al capitalismo de la era industrial, centrado en la explotación de las materias primas naturales y que utilizaba a las personas como mano de obra, en el capitalismo de vigilancia la materia prima son las propias personas (fuentes de información); sus datos obtenidos a partir de la vigilancia del comportamiento de las personas para predecir sus comportamientos futuros, que posteriormente son monetizados a través de su venta a terceros.

En la película *Sneakers* (1992, traducida en España como *Los Fisgones*), cuyo argumento trata de un grupo de expertos informáticos que, por encargo de una agencia secreta, roban un dispositivo capaz de decodificar cualquier sistema, hay un diálogo entre *Marty Bishop* (Robert Redford) y *Cosmo* (Ben Kingsley) en el que este último le dice:

> «El mundo ya no está manejado por armas, ni energía, ni dinero, sino por unos y ceros, pequeños pedazos de datos. Todo es solo electrones (…). Hay una guerra allá afuera, viejo amigo. Una guerra mundial y no se trata de quién tiene más balas. Se trata de quién controla la información. Lo que vemos y escuchamos, cómo trabajamos, lo que pensamos... ¡se trata de la información!»

La conjunción entre las actuales capacidades de recopilación, almacenamiento y procesamiento de la información por parte de las empresas, de un lado, y las obligaciones legales de conservación y facilitación de la misma a las autoridades estatales, de otro, han provocado un cualitativo salto en la investigación criminal. Hay quien relaciona esta nueva forma de investigación con la película *Minority Report* (2002), basada en un relato corto de 1956 de Philip K. DICK titulado *El informe de la minoría*, pero resulta que, mucho tiempo atrás, en la España dictatorial de 1941, Miguel FENECH escribía: «el liberalismo no establece leyes que afecten al fuero interno porque no le parece justo intervenir en la esfera íntima del hombre; el Estado totalitario no las establece porque carece de medios técnicos de vigilar su cumplimiento. Si se inventase un aparato que permitiera leer los pensamientos y descifrar las intenciones, el Estado totalitario desarrollaría en el acto una vivísima legislación interna[2]».

Hoy ya es posible afirmar que existe esa capacidad empresarial (marketing digital) de detectar tendencias, gustos y necesidades, predecir comportamientos y anticiparse a los deseos de las personas para facilitarles los productos y servicios demandados. Por ello, si los algoritmos aplicados a la optimización de la extracción de la información vertida con la navegación web (búsquedas efectuadas, páginas visitadas, compras realizadas, etc.) permiten detectar y predecir

---

[1] ZUBOFF, S. (2019). *The Age Of Surveillance Capitalism*. New York: PublicAffairs.

[2] FENECH, M. (1940). *El juez y el Nuevo Estado*. Barcelona: Bosch, p. 162, citado por MAROTO CALATAYUD, M (2013). Las redes sociales en internet como instrumento de control penal: tendencias y límites. En RALLO LOMBARTE, A., MARTÍNEZ MARTÍNEZ, R. (edit.) *Derecho y Redes Sociales*. Madrid: Civitas, pp. 427-484.

tales comportamientos, debemos convenir que la recolección y cruce inteligente de los datos generados con motivo de las comunicaciones e informaciones compartidas a través de la red también permiten reconstruir los movimientos e interacciones de las personas. De este modo, y como quiera que el principal objetivo de cualquier investigación criminal consiste en obtener información (averiguar y hacer constar, con el mayor detalle y exhaustividad posible —dentro de los márgenes legales—, la perpetración de los delitos con todas las circunstancias, según el art. 299 LECrim), la clave de cualquier investigación pasará por la utilización de aquellas herramientas legales que permitan a las autoridades acceder a la mayor cantidad de información relacionada con los hechos objeto de indagación, de una manera rápida, eficiente y con un sacrificio proporcionado de los derechos de los sujetos sobre los que recae la investigación.

Según cuenta la mitología griega, Ariadna entregó a Teseo un ovillo de hilo de oro para que lo desenrollara según se adentraba en el laberinto del Minotauro, de modo que luego pudiera volver tras sus pasos y encontrar la salida. Hoy en día, más que en Teseo, nos hemos convertido en la versión moderna de Hansel y Gretel; constantemente vamos dejando "migas de pan" en múltiples formatos digitales, a partir de las diversas interacciones que llevamos a cabo (conexiones y comunicaciones a través de nuestros teléfonos móviles y otros dispositivos inteligentes, navegación web, uso de servicios basados en la geolocalización, compras online, tránsito en lugares videovigilados, etc.). El sueño de cualquier investigador sería localizar ese ovillo de hilo de oro que, recogiéndolo como si fuera el sedal de una caña de pescar, le permitiera identificar y aprehender al autor de un hecho delictivo.

Con tal finalidad, los verdaderos avances legislativos en materia de empleo de la tecnología para la recolección de información utilizable posteriormente con fines probatorios en el proceso penal han venido de la mano de normas sectoriales extraprocesales, *de puntillas y por vericuetos diversos*[3], cuyo principal exponente europeo lo constituiría 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, alumbrada con el firme propósito de facilitar la prevención, investigación, detección y enjuiciamiento de los delitos.

2. «CRÓNICA DE UNA MUERTE ANUNCIADA»: EL RECHAZO EUROPEO A UNA CONSERVACIÓN SISTEMÁTICA E INDISCRIMINADA DE DATOS

En la construcción del Espacio Europeo de Libertad, Seguridad y Justicia, una de las grandes controversias aún por resolver se centra en cómo cohonestar las enormes posibilidades que la tecnología ofrece en materia de tratamiento informático de datos personales a gran escala (*Big Data*) y su empleo para la protección de la seguridad pública, la defensa o el orden público con la debida protección de los derechos fundamentales de los ciudadanos reconocidos en el Convenio Europeo de los Derechos Humanos y en la Carta de Derechos Fundamentales de la UE.

Por ello, y como si se tratara del personaje de *Santiago Nasar*, la narración de la historia de la Directiva 2006/24/CE bien podría comenzar con la frase «el día que la iban a anular…».

Distintas voces jurídicas autorizadas criticaron, desde su génesis, el sistema de conservación generalizada de datos de comunicaciones electrónicas articulado en dicho régimen e ideado con la vista puesta en los atentados terroristas que sacudieron Madrid y Londres en los años anteriores a su gestación. Basta echar un vistazo, por ejemplo, a las críticas vertidas en el Informe de la Comisión al Consejo y al Parlamento de evaluación sobre la Directiva de 18 de abril de 2011; a las dudas que la misma le suscitaban al Supervisor Europeo de Protección de Datos, en su Dictamen de 23 de septiembre de 2011; a las valoraciones contenidas en los Dictámenes del Grupo de Trabajo del art. 29 en dicha materia; así como a los pronunciamientos recogidos en las declaraciones de inconstitucionalidad por parte de diversos Tribunales Constitucionales de los Estados miembros sobre las leyes de transposición de aquélla, para darse cuenta de que más pronto o más tarde tendría que acometerse una importante reforma o

[3] PÉREZ GIL, J. (2005). Entre los hechos y la prueba: reflexiones acerca de la adquisición probatoria en el proceso penal, *Revista Jurídica de Castilla y León*. n.º 14. enero 2008, p. 233 y ss.

cambio de rumbo[4]. Y, en efecto, aunque la Directiva aguantó el primer envite —STJUE *Irlanda c. Parlamento Europeo* (C-301/06), de 10 de febrero de 2009—, no sobrevivió a la STJUE *Digital Rights Ireland y otros* (C-293/12) y *Seitlinger y otros* (C-594/12), de 8 de abril de 2014, que declaró su invalidez por permitir una injerencia desproporcionada en los derechos al respeto de la vida privada y familiar y a la protección de datos de carácter personal, reconocidos por la Carta de Derechos Fundamentales de la Unión Europea.

A partir de ahí, muchos Estados reformaron sus legislaciones domésticas en materia de conservación de datos y cesión a las autoridades estatales, anudándolas, entonces, al artículo 15, apartado 1, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002[5], relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que habilita a los Estados miembros a adoptar «medidas legales» para excepcionar los derechos contenidos en la misma —principalmente, la imposición de obligaciones de conservación temporal de determinados datos y su cesión a las autoridades— por razones de protección de la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos.

Pero la doctrina asentada por el TJUE en la posterior Sentencia *Tele2 Sverige* (C-203/15) y *Watson y otros* (C-698/15), de 21 de diciembre de 2016, no deja margen para sostener la adecuación de tales leyes nacionales —entre las cuales debemos incluir la española— a los estándares de protección de los derechos fundamentales reconocidos en los arts. 7, 8, 11 y 52.1 de la Carta[6]. Y a dicha jurisprudencia debemos añadir las conclusiones de los Abogados Generales a los asuntos C-511/18 y C-512/18, C-520/18, C-623/17 y C-746/18, referidas todas ellas a cuestiones prejudiciales que sometían a examen distintas regulaciones de los Estados miembros en materia de conservación de datos de comunicaciones electrónicas, hechas públicas a comienzos de enero de 2020. En todas ellas, la opinión de los Abogados Generales aboga por declarar su incompatibilidad con el Derecho de la Unión Europea (en particular, con la Directiva 2002/58/CE y la Carta de Derechos Fundamentales de la Unión Europea).

Para el TJUE, la conservación de los datos constituye, por sí, una excepción al deber de garantizar la confidencialidad de las comunicaciones realizadas a través de una red pública de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público que debe ser interpretada en un modo sumamente restrictivo, y sin embargo, el sistema seguido por tales legislaciones nacionales se caracteriza por tratarse de una conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica, sin apenas diferenciación, limitación o excepción en función del objetivo que se pretende lograr.

---

[4] En este sentido, véase el excelente compendio realizado por SERRANO MASIP, M. (2012). La conservación sistemática y preventiva de datos de tráfico y localización generados por las comunicaciones electrónicas: reacciones contrarias y posible cambio de rumbo en la Unión Europea. En CASTILLEJO MANZANARES, R. (dir.) *Temas actuales en la persecución de los hechos delictivos*. Madrid: La Ley, pp. 437-500.

[5] En España, sin embargo, la norma que había traspuesto la Directiva invalidada —la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones— apenas fue objeto de ligeros retoques a través de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, lo cual dio pie a un importante debate doctrinal entre partidarios y detractores de su validez. Sin ánimo exhaustivo, los principales argumentos a favor de su validez pueden apreciarse en RODRÍGUEZ LÁINZ, J. L. (2014). Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española de conservación de datos relativos a las comunicaciones. *Diario La Ley*, núm. 8308, de 12 de mayo de 2014. En contra, véanse los argumentos que sostienen la nulidad de nuestra legislación expuestos por ENCINAR DEL POZO, M. A. (2014). La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones. *SEPIN Top Jurídico, Nuevas Tecnologías*, octubre 2014. Referencia: SP/DOCT/18682.

[6] Un excelente debate doctrinal sobre el impacto de dicha STJUE en nuestra legislación puede verse en la Encuesta Jurídica del portal jurídico SEPÍN publicada en Febrero de 2017 (Referencia: SP/DOCT/22410): *La Sentencia del TJUE de 21 de diciembre de 2016 que declara contraria al Derecho de la UE una Ley que regule la conservación de datos, ¿en qué grado afecta a la Ley 25/2007, de Conservación de Datos y a la reciente reforma de la LECrim., en lo que a la cesión de datos se refiere, respecto a la investigación de delitos cometidos a través de Internet?*.

La obra «Roma: Auge y caída de un imperio», de Simon BAKER, narra la historia del imperio romano, desde su expansión por el mar Mediterráneo hasta su ocaso a manos de los pueblos bárbaros del norte de Europa. De igual modo, la historia de las investigaciones penales basadas en esa inagotable fuente de información como son los datos externos de las comunicaciones electrónicas también tendría un auge —representado por la aprobación de la Directiva de 2006— y un ocaso —representado por la restrictiva jurisprudencia aquí examinada—.

En nuestra opinión, el elevado listón impuesto por el TJUE a la hora de señalar los criterios que deberían ser tenidos en cuenta a la hora de regular un sistema de conservación preventiva de datos relativos a las comunicaciones electrónicas de los usuarios de tales servicios (v. gr., un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave) dificulta enormemente el surgimiento de una normativa, nacional o europea, compatible con la interpretación de la Carta Europea que realiza el TJUE. A diferencia del «acceso» o cesión a las autoridades correspondientes, más maleable a la hora de ser sometido a específicos criterios subjetivos, objetivos, materiales y temporales que justifiquen la idoneidad, necesidad y proporcionalidad de la injerencia, la «conservación» resulta ser mucho más compleja de someterse a los parámetros indicados por el Tribunal de Luxemburgo. Y las propuestas vertidas en las Conclusiones presentadas en enero de 2020 apuntan en esa misma y peligrosa dirección de convertir la regulación de los perímetros de conservación de datos de comunicaciones electrónicas en una tarea titánica para los legisladores nacionales.

3. «LOS CUATRO JINETES DEL APOCALIPSIS»: LA DEFINITIVA DEFENESTRACIÓN DE LA LEY ESPAÑOLA SOBRE CONSERVACIÓN DE DATOS RELATIVOS A LAS COMUNICACIONES ELECTRÓNICAS[7]

En la obra de Vicente BLASCO IBÁÑEZ, ambientada a comienzos del siglo XX en la Europa de la Primera Guerra Mundial, *Tchernoff* les habla a sus compañeros sobre los cuatro jinetes que precedían la aparición de la bestia en la visión del apóstol San Juan. El Apocalipsis es el último libro del Nuevo Testamento que profetiza, según la tradición cristiana y a través de un marcado simbolismo, el fin del mundo. Pero su etimología griega también significa "revelación".

En la Europa del siglo XXI, en esa nueva guerra por el control de la información a la que aludía *Cosmo*, las cuatro conclusiones presentadas por los Abogados Generales del TJUE, el Sr. Manuel Campos Sánchez-Bordona y el Sr. Giovanni Pitruzzella[8], bien merecen ambos sustantivos. De una parte, y junto con la jurisprudencia condensada en las sentencias *Digital Rights, Tele2 Sverige y Watson* y *Ministerio Fiscal*, representan el fin de las leyes nacionales inspiradas por la Directiva de 2006, y muy especialmente, de la Ley 25/2007, tal y como está actualmente configurada en nuestro país[9]. De otra parte, nos revelan el camino a seguir a la hora de acometer la necesaria reforma de nuestro ordenamiento jurídico referido a la conservación de datos generados o asociados a comunicaciones y su oportuna cesión a las autoridades encargadas de la investigación criminal para cumplir con los estándares recogidos en los arts. 7, 8, y 52 de la Carta Europea de Derechos Fundamentales (CEDFUE) y el art. 8 CEDH.

A diferencia de la STJUE *Ministerio Fiscal*, en estas cuestiones prejudiciales sí que se pregunta directamente si es compatible o no con el Derecho de la Unión una normativa nacional

[7] Así se titula el trabajo publicado por RODRÍGUEZ LÁINZ en el *Diario La Ley*, núm. 8901, de 16 de enero de 2017, que describe nítidamente el peligro al que nos enfrentamos.

[8] El primero las presentó el 15 de enero de 2020 y se refieren a los Asuntos C-511/18 y C-512/18, C-520/18 y C-623/17. El segundo las comunicó el 20 de enero de 2020 y se refieren al Asunto C-746/18. A la fecha de entrega del presente trabajo, todas ellas aún eran objeto de examen por el TJUE. No obstante, su examen será conjunto, pues entre las mismas existen constantes remisiones a la opinión de uno u otro Abogado General.

[9] Siempre hemos defendido su excesiva desproporcionalidad, como puede apreciarse en 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*, nº 75, Octubre 2010.

que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar de manera generalizada e indiferenciada los datos de conexión, y en su caso, datos de tráfico y de localización, en términos muy semejantes a los configurados en la Ley 25/2007, de modo que sus conclusiones serán directamente trasladables a la configuración de nuestra legislación, sin que pueda seguir manteniéndose una pretendida autonomía de nuestra controvertida ley de 2007. Resulta muy loable la defensa numantina que tanto el Tribunal Supremo como ciertos autores hacen del sistema español de conservación de datos de comunicaciones electrónicas, pero el mismo no puede seguir considerándose un reino de taifas inmune a los parámetros y garantías exigidas por el Tribunal de Luxemburgo. Como analizaremos al final del presente trabajo, tan sólo es cuestión de tiempo que el Alto Tribunal Europeo sea requerido para pronunciarse sobre la norma española, e incluso es factible que ni tan siquiera se plantee una cuestión prejudicial y cualquier órgano nacional la declare inaplicable por resultar incompatible con el Derecho Europeo, de modo que, como más vale prevenir que curar, el legislador español debería poner en práctica aquel refrán de «cuando las barbas de tu vecino veas pelar,…».

3.1. El caballo blanco: la *Victoria* del Ministerio Fiscal en el Asunto C-207/16

Ante la libertad otorgada por la Directiva 2006/24/CE para que los Estados definieran la noción de «delitos graves» para cuya investigación, detección y enjuiciamiento procedía el deber de conservación, el legislador español optó por traducir dicha noción como los *delitos graves contemplados en el Código Penal o en las leyes penales especiales*. Craso error: la interpretación literal de tal precepto por diversos Juzgados de Instrucción y Audiencias Provinciales provocó serios quebraderos de cabeza a la Fiscalía, que se tuvo que emplear a fondo para evitar que tal interpretación *ad pedem litterae*, conforme al concepto de delito grave contenido en el art. 33 CP, dejara impunes múltiples delitos cometidos a través de Internet, cuando el delito objeto de investigación no alcanzaba ese límite penológico[10].

No es ahora el momento de llamar la atención, una vez más, sobre los escasos avances efectuados en el Espacio Judicial Europeo en determinadas parcelas como, por ejemplo, la distribución de la competencia judicial entre los Estados miembros en materia penal o la delimitación a nivel europeo de la noción de «delito grave». Precisamente por ello, la STJUE *Ministerio Fiscal* puede ser considerada una victoria para las autoridades españolas, pues consiguió salvar ese *match ball* consistente en circunscribir la proporcionalidad de la injerencia únicamente a la pena aparejada al delito investigado. Para el Tribunal, y conforme al principio de proporcionalidad, "cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general" (apartados 54 a 57), y concluyó que la identificación de los titulares de las tarjetas SIM activadas durante un período de doce días con el número IMEI del teléfono móvil sustraído no debía considerarse, bajo esa óptica, como una injerencia «grave».

Sin embargo, no debemos lanzar las campanas al vuelo; dicha victoria debe ser tildada de pírrica. En primer lugar, y como bien apunta el AG Campos Sánchez-Bordona en sus Conclusiones presentadas en el Asunto C-520/18 (apartados 66 y 67), porque en el asunto zanjado por la sentencia *Ministerio Fiscal* "no se planteaba si los datos personales objeto de acceso habían sido conservados por los proveedores de comunicaciones electrónicas de conformidad con las condiciones contempladas en el artículo 15.1 de la Directiva 2002/58, interpretadas a la luz de los artículos 7 y 8 de la Carta (…). De ahí que la lectura de la sentencia *Ministerio Fiscal* no permita deducir ningún cambio en la doctrina del Tribunal de Justicia sobre la incompatibilidad con el derecho de la Unión de un régimen nacional que autoriza el almacenamiento generalizado e indiferenciado de datos, en el sentido de la sentencia *Tele2 Sverige y Watson*". Y en segundo lugar, porque el TJUE dejó expresamente sin contestar las dos importantes cuestiones planteadas por la Audiencia Provincial de Tarragona. A saber: 1ª) si la gravedad del delito como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los arts. 7 y 8 de la Carta puede identificarse únicamente en atención a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta

[10] Un análisis de dicho desaguisado, y propuestas para solventar la cuestión, se recogen en ORTIZ PRADILLO, J. C. (2013). *Problemas procesales de la ciberdelincuencia*. Madrid: Colex, pp. 236-240.

delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos, y 2ª) si se ajustaría a los principios constitucionales de la Unión, un umbral mínimo de tres años de prisión.

En efecto, aunque el TJUE reconoce expresamente (aptdo. 50) que la cuestión planteada por la AP de Tarragona pretendía resolver "qué elementos es preciso tener en cuenta para apreciar si los delitos respecto de los cuales puede autorizarse a las autoridades policiales, a efectos de investigación de un delito, a acceder a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas son de una gravedad suficiente para justificar la injerencia que supone tal acceso en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta, tal como los interpreta el Tribunal de Justicia en sus sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, y Tele2 Sverige y Watson y otros", podemos concluir que el Tribunal se fue por los cerros de Úbeda y no respondió directamente a dicha cuestión, ante lo cual sólo nos queda extraer la siguiente y provisional conclusión, y en negativo, sobre la noción de «injerencia grave»: Deberán ser calificadas como tales aquellas actuaciones que "permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan[11].

3.2. El caballo rojo: la *Guerra* por delimitar el marco jurídico aplicable a la conservación de datos

En la STJUE, Gran Sala, de 30 de mayo de 2006 (Asuntos acumulados C-317/04 y C-318/04), se puso el acento en la transmisión de los datos personales recopilados —intercambio de datos PNR entre la Comunidad Europea y los Estados Unidos de América— de cara a admitir su exclusión del régimen de la Directiva 95/46/CE, precisamente porque dicha transmisión internacional se estimaba una actividad propia de los Estados a nivel internacional, de modo que si bien la recopilación se lleva a cabo por operadores privados con fines mercantiles, la transferencia "se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública" (aptdo. 58).

Esta Sentencia *Parlamento/Consejo y Comisión* elaboró una doctrina diferenciadora entre la cláusula de exclusión y las cláusulas de restricción o limitación de la Directiva 95/46 (análogas a las de la Directiva 2002/58) que han servido de base argumental para que los gobiernos trataran de excluir esos regímenes de retención y conservación de datos electrónicos de la aplicación de la Directiva 2002/58 y del Derecho de la UE en materia de protección de datos personales y del resto de Derechos Fundamentales, al tener por objeto la seguridad pública, la defensa, la seguridad del Estado y a las actividades del Estado en materia penal. Sin embargo, las Conclusiones sostienen lo contrario, al considerar que el régimen de conservación de datos de comunicaciones electrónicas impuesto a los proveedores de acceso sí quedan bajo la regulación de la Directiva 2002/58 y del Derecho de la UE y no deben considerarse como "actividades propias de los Estados o de las autoridades estatales, ajenas a los ámbitos de actividad de los particulares" a las que se refirió la STJUE *Parlamento/Consejo y Comisión*.

Los Abogados Generales Campos Sánchez-Bordona y Pitruzzella entienden que la noción de "seguridad nacional" a los efectos de excluir la aplicación de la Directiva 2002/58 debe ser entendida de un modo excepcional, como por ejemplo, cuando se trate de técnicas de recopilación de información que sean aplicadas directamente por el Estado, pero no cuando se trate de normas que regulen las actividades de los proveedores de servicios de comunicaciones electrónicas imponiéndoles obligaciones específicas a tales empresas privadas. Esto es, tal exclusión debe entenderse referida únicamente a "las competencias de los Estados miembros en materia de seguridad nacional, cuando las ejercen *de manera directa y por sus propios medios*. Por el contrario, cuando, incluso por esas mismas razones de seguridad nacional, se requiere el concurso de particulares, a quienes se imponen ciertas obligaciones, esta

[11] Véanse el aptdo. 27 de la Sentencia *Digital Rights*, el aptdo. 99 de la Sentencia *Tele2 Sverige y Watson y otros*, y el aptdo. 60 de la Sentencia *Ministerio Fiscal*. En el mismo sentido, OROMÍ I VALL-LLOVERA, S. (2020). Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE, *Revista de Internet, Derecho y Política*, N.º 31 (Octubre, 2020), p. 5.

circunstancia determina la entrada en un ámbito (la protección de la privacidad exigible a esos actores privados) regido por el derecho de la Unión[12]".

En sus conclusiones, se defiende la posibilidad de llevar a cabo una interpretación integradora de la Sentencia *Parlamento/Consejo y Comisión* con la Sentencia *Tele2 Sverige y Watson* que permita una relación armónica y sistemática entre cláusulas de exclusión y cláusulas de restricción en función de diversos criterios. Por una parte, cabe apreciar que, si en la primera Sentencia se ponía el foco en la dimensión internacional (intercambio de información con fines de protección de la seguridad nacional), en la segunda se incide en el carácter mercantil de la actividad (la retención y conservación de datos en manos de empresas privadas). Por otra parte, también se destaca la "suficiente disparidad" existente entre el art. 3.2 de la Directiva 95/46 y el art. 1.3 de la Directiva 2002/58; la primera excluía el tratamiento de datos que tenga por objeto la seguridad del Estado, con independencia del sujeto que lo llevara a cabo, mientras que la segunda lo hace con las actividades dirigidas a preservar la seguridad estatal y únicamente cuando dicha actividad sea una actuación material de los propios poderes públicos, esto es, "actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares", no pudiendo admitirse que esas «actividades» sean de naturaleza normativa, porque si así fuera, todas las disposiciones adoptadas por los Estados miembros en relación con el tratamiento de datos personales quedarían fuera del ámbito de la Directiva 2002/58, a poco que pretendieran justificarse como necesarias para garantizar la seguridad del Estado[13].

Vistas así, estas conclusiones podrían considerarse un importante varapalo para los intereses estatales. Ahora bien, las mismas señalan algunas válvulas de escape que, a buen seguro, serán convenientemente aprovechadas por los Estados en sus reformas internas.

En primer lugar, se alude expresamente y como "orientación" a la Decisión Marco 2006/960/JAI, del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, a los efectos de excluir de la normativa sobre privacidad y comunicaciones electrónicas aquellas actividades estatales de obtención de información y recogida de inteligencia criminal. Ello supone abrir la puerta a una importante y positiva baza en manos de los Estados miembros para conformar sistemas propios de recolección y almacenamiento de datos personales que se convertirán en vitales en la lucha contra el crimen. Me refiero a la creación del «Gran Hermano» policial en la Unión Europea: el denominado "marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración[14]", gestionado por la Agencia EU-LISA, y consistente en la creación de un portal europeo de búsqueda (PEB), un servicio de correspondencia biométrica compartido (SCB compartido), un registro común de datos de identidad (RCDI) y un detector de identidades múltiples (DIM) que aglutine la información actualmente recogida en el Sistema de Entradas y Salidas (SES), el Sistema de Información de Visados (VIS), el Sistema Europeo de Información y Autorización de Viajes (SEIAV), Eurodac, el Sistema de Información de Schengen (SIS), y el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN). Ello supone un gigantesco avance en la obtención y cruce inteligente de información que sea directamente creada o recopilada por las autoridades estatales, pues dicho marco de interoperabilidad de los sistemas de información puede ser empleado, no sólo para mejorar los controles en las fronteras exteriores, mejorar la aplicación de la política común de

---

[12] Vid. aptdo. 85 Asuntos acumulados C 511/18 y C 512/18 y aptdo. 24 Asunto C 623/17. En el aptdo. 43 del Asunto C 746/18 se señala también que, tal y como se declaró por el TJUE en la Sentencia *Ministerio Fiscal*, no sólo están incluidas en el ámbito de aplicación de dicha Directiva aquellas medidas que obligan a los proveedores de servicios de comunicaciones electrónicas a conservar los datos de tráfico y los datos de localización, sino también aquellas medidas relativas al acceso de las autoridades nacionales a los datos conservados por dichos proveedores, pues la protección de la confidencialidad de las comunicaciones electrónicas y de sus datos de tráfico *se aplica a las medidas adoptadas por todas las personas distintas de los usuarios, ya sean personas físicas o entidades privadas o públicas y tiene como objetivo evitar "[todo] acceso" no autorizado a las comunicaciones, incluido "todo dato relativo a esas comunicaciones", para proteger la confidencialidad de las comunicaciones electrónicas*.

[13] Vid. aptdos 73 y ss. Asuntos acumulados C 511/18 y C 512/18.

[14] Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019. DOUE L 135/85, de 22 de mayo.

visados y prestar asistencia en el examen de las solicitudes de protección internacional, prevenir y combatir la inmigración ilegal y, en general, alcanzar un elevado nivel de seguridad en el Espacio de libertad, seguridad y justicia de la Unión, sino que también se considera un objetivo legítimo su empleo de cara al "mantenimiento de la seguridad pública y del orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros, y *la prevención, detección e investigación de los delitos de terrorismo u otros delitos graves*[15]".

En segundo lugar, y si bien se recuerda que la doctrina de la Sentencia *Tele2 Sverige y Watson* resulta igualmente aplicable a la lucha contra el terrorismo, se deja abierta la posibilidad de que "en situaciones propiamente excepcionales, caracterizadas por una amenaza inminente o por un riesgo extraordinario que justifiquen la declaración oficial de la situación de emergencia en un Estado miembro, la legislación nacional contemple, por un tiempo limitado, la posibilidad de imponer una obligación de conservación de datos tan amplia y general como se considere imprescindible[16]". Es decir, se abre la puerta a la posibilidad de idear regímenes legales extraordinarios enfocados a una conservación selectiva en lo material (datos) pero más amplia en lo personal (sujetos afectados), temporalmente delimitada, y con arreglo a condiciones y procedimientos que aseguren y diferencien ese carácter extraordinario y correlacionen los datos cuya conservación se establece con las amenazas para la seguridad pública que lo motivan. Y en esa regulación excepcional de emergencia reconducida a «amenazas graves y persistentes a la seguridad nacional y, en particular, el riesgo de terrorismo», se permite que los Estados miembros den una respuesta *que no tiene por qué ser idéntica*[17].

3.3. El caballo negro: el *Hambre* de no poder acudir al mayor granero de información

Desde los orígenes de los tiempos, han sido muchas y muy variadas las fórmulas utilizadas a la hora de indagar y esclarecer los hechos y castigar al culpable y el uso de la tecnología también ha estado siempre presente, de una u otra manera. No en vano, si en el plano criminal, la actual Sociedad Digital y la hiperconectividad que la caracteriza ha sido bien recibida por los criminales para desplegar nuevas conductas y servirse de la arquitectura de la Red como vehículo comisivo, también ha sido aprovechada por las autoridades policiales para aumentar su capacidad investigadora, gracias a lo que hemos denominado como la «transversalidad de la prueba electrónica[18]».

En el terreno de la Criminalística, se han diferenciado tres etapas en el ámbito de la investigación policial[19]: La primera —época primitiva—, arbitraria o de inexistencia de una verdadera investigación policial en la forma como en la actualidad se la conoce, hasta finales del siglo XVIII; la segunda fase —etapa intermedia—, de iniciación a la Técnica Policial, que alcanza desde el fin de la anterior hasta finales del siglo XIX; y la tercera fase —Policía Científica—, que se corresponde con el siglo XX. En nuestra opinión, debemos añadir una cuarta etapa, coincidente con el inicio del nuevo milenio, caracterizada por el uso generalizado de los más avanzados instrumentos tecnológicos y metodologías científicas por parte de las Fuerzas y Cuerpos de Seguridad del Estado, especialmente en labores de investigación y seguimiento —Tecnovigilancia— y ello a pesar de la falta de una legislación suficiente y moderna sobre la materia.

---

[15] Considerando nº9 del Reglamento.

[16] Véanse los aptdos. 104 y ss. de las Conclusiones a los Asuntos C-511 y 512/18 y aptdos. 105 y ss. de las Conclusiones al Asunto C-520/18.

[17] Vid. aptdos. 103 y siguientes de los Asuntos acumulados C-511/18 y C-512/18.

[18] Es la regla contenida en el art. 14.2 del Convenio de Budapest en materia de Ciberdelincuencia, que permite la utilización de los especiales poderes de investigación para "la obtención de pruebas electrónicas de cualquier delito". Sobre ello, vid. ORTIZ PRADILLO, J. C. (2012). Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica. En: PÉREZ GIL (coord.), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*. Madrid, ed. La Ley, pp. 267-310.

[19] CABEZAS, P. (2010). La investigación del crimen a través de los tiempos. Tesis doctoral. Universitat Autònoma de Barcelona. Accesible en la dirección URL https://www.educacion.gob.es/teseo/imprimirFicheroTesis.do?idFichero=FIHxYNhGkts%3D. Fecha de consulta: 7 de abril de 2020.

Como quiera que la tecnología está presente en casi cualquier conducta humana, la información creada o intercambiada gracias a los dispositivos utilizados a diario constituye una valiosísima fuente de prueba para investigar y esclarecer cualquier clase de delito, sea o no de los denominados "delitos informáticos"; esto es, de cara a incrementar exponencialmente las capacidades policiales para la averiguación de las conductas criminales, los datos y metadatos producidos con motivo de servicios de telecomunicaciones tienen un valor casi similar a los tesoros que Hércules guardó, según cuentan las leyendas de la ciudad de Toledo, en una enorme cueva.

Ese enorme tesoro o granero que representan los datos conservados en poder de las operadoras de telecomunicaciones y de las empresas tecnológicas de prestación de servicios de la Sociedad de la Información, a la hora de localizar rastros digitales que permitan identificar al delincuente y relacionarlo con el hecho punible, puede echarse a perder o no ser debidamente utilizado si las condiciones de acceso a los mismos se convierten en «*27 cerrojos*[20]» en forma de criterios objetivos, subjetivos, geográficos, materiales y temporales, que los Estados deberán saber regular a la hora de instaurar un «acceso limitado» compatible con la interpretación de los Derechos Fundamentales contenidos en la Carta Europea. Visto así, no sólo la información almacenada será equiparable a los tesoros de Hércules, por la dificultad de poder acceder a los mismos, sino que la titánica labor de los Estados de conseguir aprobar una normativa nacional sobre el acceso a dichos datos, conforme con dicha jurisprudencia del TJUE y de las Conclusiones de enero de 2020, bien podrá calificarse como las doce tareas de Hércules.

Aún con todo, en esta carrera de obstáculos impuesta por el Alto Tribunal de la Unión Europea existe una dificultad aún mayor a la facilitación de un "acceso limitado": idear y regular específicos criterios de proporcionalidad limitativos de la propia recolección y retención (lo que el Tribunal de Luxemburgo denomina «conservación selectiva»). En los delitos cometidos a través de o con ayuda de las comunicaciones electrónicas, principalmente, los datos en poder de las operadoras de acceso a la Red y de servicios informáticos constituyen el «condensador de fluzo» del que se alimenta el DeLorean con el que el investigador policial viaja al pasado en busca de conductas e interacciones pasadas, gracias a los trazos dejados por tales comunicaciones o conexiones (dirección IP utilizada, datos identificativos del terminal empleado, interacciones con puntos de conexión a la red como estaciones BTS o puntos de acceso Wi-Fi, etc.), de modo que la imposición de un régimen excepcional, selectivo y limitado en cuanto a los datos a conservar y sus periodos temporales supone un auténtico torpedo en la línea de flotación de los actuales sistemas nacionales de retención de datos, a mi modo de ver, difícil de reparar únicamente por vía interpretativa, exigiendo una importante reforma legislativa en los países miembros de la Unión Europea.

Éste es el principal caballo de batalla actual: Para el TJUE, la mera conservación, al constituir un tratamiento de datos de carácter personal y una excepción al deber de confidencialidad de las comunicaciones, ya es de por sí una injerencia en los Derechos Fundamentales a la privacidad y a la protección de datos de carácter personal garantizados por los arts. 7 y 8 CEDFUE que exige interpretarse en sentido estricto. Y en las Conclusiones que ahora estamos analizando, los Abogados Generales no sólo proponen confirmar la jurisprudencia del TJUE que consagra el carácter desproporcionado de una conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados, de manera sistemática y continuada, sin ninguna excepción —tal y como sucede en España—; también advierten, como estocada final, que "Las exigencias en materia de «conservación selectiva» y de «acceso limitado» deben entenderse como requisitos cumulativos y no alternativos", rechazando que los Estados puedan compensar una conservación extendida o indiscriminada a cambio de mayores controles respecto al acceso a los mismos[21]. Tal y como explicita el AG Campos Sánchez-Bordona, la conservación y el acceso a los datos constituyen *dos tipos distintos de interferencia*, de modo que, aun cuando la conservación de datos tenga su razón de ser de cara a un posible acceso posterior de las autoridades competentes, cada una de esas injerencias debe justificarse por separado, mediante un examen específico a la luz del

[20] Las mismas leyendas cuentan que Hércules impuso como tradición que cada nuevo rey toledano colocase un cerrojo en el Torreón que daba entrada a la cueva, hasta el Rey don Rodrigo, el último de los reyes godos, forzó los 27 cerrojos dispuestos por sus predecesores. Y todos sabemos cómo prosiguió la historia de la península ibérica tras ese *forzamiento* de la cava.
[21] Vid., por todos, los apartados 75 y siguientes del Asunto C-520/18.

objetivo perseguido, y someterse a criterios objetivos y proporcionados con la gravedad de la injerencia que dicho almacenamiento supone.

Sin duda, esta conclusión es, como digo, el principal torpedo en la línea de flotación de la legislación española, pues aunque el nuevo régimen incorporado a la LECrim en sus arts. 588 bis y siguientes pudiera llegar a superar el filtro de requisitos y garantías para ser considerado un ejemplo de "acceso limitado", la «*materia prima*» de la que se nutren las autoridades encargadas de las investigaciones penales se sigue basando en un régimen de conservación indiscriminada. De hecho, la legislación belga sometida a cuestión prejudicial en el Asunto C-520/18 resulta claramente similar a la ley española y la opinión del AG no deja lugar a dudas: "la legislación belga impone a los operadores y proveedores de servicios de comunicaciones electrónicas la *obligación, general e indiferenciada*, de conservar los datos de tráfico y de localización (…). El período de conservación es de doce meses, en general: no se contempla ninguna limitación temporal en función de las categorías de datos conservados. (…) Esa obligación de conservación general e indiferenciada rige de manera permanente y continuada. (…) una obligación de estas características no se ajusta a la jurisprudencia del Tribunal de Justicia, de manera que no puede reputarse compatible con la Carta[22]".

Excluidos de la investigación criminal esos datos electrónicos conservados en cumplimiento de la legislación derivada de la Directiva 2006/24/CE, las autoridades sólo podrán reclamar aquéllos que hayan sido generados o conservados por las operadoras "por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación" (art. 588 ter j.1 LECrim), con los límites temporales marcados por los arts. 6 y 9 de la Directiva 2002/58/CE, o aquellos datos o informaciones concretas incluidas en un sistema informático de almacenamiento en poder de las entidades que ofrecen servicios de la Sociedad de la información pero no se encuentran sujetas a los deberes de conservación de la Ley 25/2007 (art. 588 octies LECrim).

Pero no todo está perdido. El refranero español es muy sabio, y ante la imposibilidad de acudir a ese valioso granero constituido por los datos de tráfico conservados en virtud de la Ley 25/2007, *el hambre agudiza el ingenio*. Los investigadores optarán por acudir a otros caladeros en busca de otros formatos y tipologías de datos derivados de interacciones telemáticas, como por ejemplo, los metadatos generados con motivos de intercambios de información, los datos de conexión e intercambio automático de información entre dispositivos, o los datos derivados de servicios de geolocalización "que se produzcan con independencia del establecimiento o no de una concreta comunicación (art. 588 ter b.2 LECrim)". Y es que, mientras que la Ley 25/2007 fijó en su art. 3.f) el deber de conservar los datos de localización "al inicio de la comunicación", la reforma de la LECrim en 2015 permite a las autoridades acceder a muchos otros datos de conexión e intercambio automático de información con las estaciones BTS sin que exista una «comunicación» a través del teléfono móvil[23].

Como ejemplo concreto, sabemos que Google recopila tales datos a través de la opción «historial de ubicaciones», e incluso cuando dicha opción está desactivada, a través de otras interacciones que llevamos a cabo con nuestro terminal móvil (búsquedas a través de su navegador o uso de sus múltiples aplicaciones, como por ej., *Google Maps, El Tiempo,…*).

---

[22] Vid. apartados 125 y 126 de las conclusiones al Asunto C-520/18.

[23] Por ejemplo, los denominados *datos de stand by*, o cobertura sin comunicación, aunque el periodo de conservación de estos datos, salvo que medie orden judicial, suele ser de unas 72 horas. Véase, PÉREZ GIL, J. (2010). El nuevo papel de la telefonía móvil en el proceso penal. Ubicación y perfiles de desplazamiento. En: *El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar probar el delito*. Madrid: La Ley, p. 200). Por su parte, RODRÍGUEZ LÁINZ, J. L. (2013). Internet de los objetos y secreto de las comunicaciones. *Diario La Ley*, núm. 8034, también afirma que la nueva regulación ha incluido "importantes novedades que atañen a la posibilidad de interceptación de la información que de forma automática se transmite entre terminales y estaciones BTS u otros dispositivos que canalizan las comunicaciones para garantizar la continuidad y calidad del servicio. Se trata de una transferencia de información que a través en esencia de canales de control o señalización, descritos como tales en el art. 39.5 a), j) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones —LGT—, nos permitirá obtener información en tiempo real, sobre estado de funcionamiento del dispositivo y geolocalización, sin necesidad de esperar a que una comunicación tenga por origen o destino el dispositivo objeto de seguimiento".

Precisamente por ello, y cuando los datos de triangulación de las antenas BTS utilizadas por el terminal de un sujeto investigado no resultan concluyentes para concretar su ubicación en un determinado momento, la información que posee Google y otras empresas del sector tecnológico sí sería indispensable para la resolución de un hecho delictivo[24].

En el sector digital, el modelo de negocio de muchas empresas se basa en la extracción y recolección de la información facilitada voluntariamente por sus usuarios o generada por la propia configuración de los equipos o por la estructura de la Red (la denominada minería de datos), como sucede con los servicios de ubicación geográfica. Me refiero, por citar un ejemplo muy concreto, a todas las aplicaciones enfocadas a compartir prácticas deportivas (*Strava, Endomondo, Runtastic, Wikiloc,…*) que registran, con una aplicación de seguimiento GPS, las rutas seguidas, la velocidad media y máxima, calorías consumidas, etc., y a través de sensores conectados a dicha aplicación se pueden guardar datos tales como la frecuencia cardíaca, temperatura corporal, la cadencia y la potencia. De acuerdo con sus términos y condiciones de privacidad, Strava reconoce recopilar, junto con la información sobre la geolocalización facilitada durante el uso de la app en entrenamientos, los datos (fecha, hora, dirección IP, el tipo de explorador, el proveedor de servicios de Internet, etc.) cuando la persona se inscribe, así como cuando ve actividades de otras personas o usa de cualquier otra forma los Servicios. Y afirma que dicha información puede ser compartida con "agencias de aplicación de la ley, públicas o gubernamentales, o litigantes privados, dentro o fuera de su país de residencia, si determinamos que dicha divulgación está permitida por la ley o es razonablemente necesaria para cumplir la ley, así como para responder a órdenes judiciales, garantías, citaciones u otros procesos legales o normativos".

Lo mismo sucede con los datos "ocultos" o "metadatos" que son inyectados en los diferentes ficheros publicados en páginas web. Gracias a ellos, las autoridades pueden localizar e identificar usuarios de la Red tras examinar, por ejemplo, los nombres de los usuarios que crearon o modificaron un determinado documento enviado a través de Internet, o las direcciones IP y de correo electrónico utilizadas para dicho envío. Específicamente referido a la geolocalización de un archivo informático, dentro de los metadatos resulta interesante tener en consideración el formato *.exif* (*Exchangeable Image File Format*) de los archivos de imagen usado por las cámaras digitales. Esas etiquetas (*tags*) de metadatos definidas en el estándar Exif contienen información sobre la fecha y hora en que se creó el archivo —se realizó la foto—, se modificó, se subió o descargó de una Red Social (que también suelen inyectar su propio código en las imágenes publicadas), pero también informan sobre la configuración de la cámara, el modelo, el fabricante, la orientación, apertura, velocidad del obturador, distancia focal, medidor de exposición, así como también la localización GPS (geoetiquetación) si se ha habilitado dicha opción. Un análisis forense de esos metadatos permitirá a los investigadores determinar el momento y las coordenadas exactas en las que se tomó una determinada fotografía, y no sólo localizar las coordenadas de la fotografía, sino también para identificar y localizar al sujeto que difundió la fotografía a través de las Redes Sociales.

Estas empresas no están sujetas a las obligaciones —ni a los plazos— de conservación impuestas por la Ley 25/2007, de modo que la anulación de la misma no impediría a las autoridades servirse de su colaboración en investigaciones criminales para saber, en virtud de los historiales conservados, si, por ejemplo, en las inmediaciones de un lugar en donde se hubiera cometido un grave hecho delictivo, y aparentemente sin testigos presenciales, había usuarios practicando deporte y utilizando estas aplicaciones de geolocalización[25], subiendo a la Red fotos y videos geoetiquetados, o desplazándose a través de los distintos servicios de movilidad basados en plataformas de alquiler de medios de transporte (patinetes, bicicletas,

[24] Al respecto, véase la noticia publicada el 17 de mayo de 2019 en el periódico *El Confidencial*. Versión online disponible en la dirección web: https://www.elconfidencial.com/tecnologia/2019-05-17/quien-provoco-incendio-sesena-clave-google_2002018/. Fecha de consulta: 20 de mayo de 2019.

[25] Un caso actual lo ha publicado el portal *iberobike*, en el que informa de que la policía autonómica del País Vasco ha sancionado por incumplir el Estado de Alarma a un ciclista que subía sus desplazamientos diarios en bicicleta a una conocida aplicación móvil de entrenamiento. Noticia publicada el 1 de abril de 2020 en la página web https://www.iberobike.com/la-policia-multa-a-un-ciclista-al-ver-en-internet-los-trayectos-que-realizadab/. Fecha de consulta: 15 de abril de 2020.

ciclomotores, vehículos VTC,…). Parafraseando el título de una conocida película, la policía podrá así saber «dónde estuvisteis el pasado verano». Y para ello, y de manera preventiva en aras a asegurar dicha información mientras consiguen el oportuno mandato judicial fundamentado en el art. 588 ter j LECrim, la policía podría servirse de la *Orden de conservación de datos* del art. 588 octies LECrim para asegurar esa información conservada sobre la localización y rutas seguidas en un pasado reciente por un determinado dispositivo móvil. El problema radicará, en tal caso, en la deslocalización de las principales empresas que ofrecen tales servicios (Strava, por ejemplo, tiene su sede en San Francisco), debiendo acudirse, en tal caso, a los instrumentos de cooperación internacional.

3.4. El caballo amarillo bayo: la *Muerte* de las investigaciones basadas en datos conservados de comunicaciones electrónicas

Como hemos indicado anteriormente, la Circular 1/2013 de la Fiscalía General del Estado alertó en su momento de los peligros de efectuar una interpretación *ad pedem litterae* del concepto de delito grave incorporado en el art. 1.1 de la Ley 25/2007 porque —decía entonces— «supone cortar de raíz la posibilidad de investigar conductas que utilizando tecnologías de la información y la comunicación y teniendo gran trascendencia social, no alcanzan por la penalidad asignada el rango de delito grave. Por ello, al margen de que los Sres. Fiscales defiendan *de lege data* la interpretación superadora de la literalidad del precepto, es a todas luces aconsejable *de lege ferenda* la modificación de la Ley 25/2007 para sustituir la expresión "delito grave" por otra que delimite el perímetro de aplicación de la Ley en términos más amplios y razonables». Y el ruego de tan necesaria reforma legal volvió a reclamarse en la Memoria anual presentada en la apertura del año judicial de 2013[26].

Si la interpretación del requisito de gravedad delictiva de la Ley 25/2007 por parte de algunos órganos judiciales nacionales hizo saltar las alarmas, eso no es nada comparado con lo que puede suceder si dicha normativa llegara a ser sometida al examen del TJUE, algo que por fortuna no sucedió con el planteamiento de las cuestiones prejudiciales que dieron pie a la Sentencia *Ministerio Fiscal*. Atendiendo a su consolidada jurisprudencia, a la que presumiblemente podrían sumarse las que resuelvan las cuestiones prejudiciales cuyas conclusiones hemos diseccionado en el presente trabajo, entendemos que la Ley 25/2007 debe ser considerada "una conservación generalizada e indiferenciada" contraria a la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea[27].

La repercusión sería brutal: se imposibilitaría hacer valer los datos obtenidos en virtud de dicha conservación como medio probatorio en cualquier proceso penal. Y tal y como advierte el AG Sr. Pitruzzella en los apartados 47 y 48 de sus conclusiones al Asunto C-746/18, "Si bien es cierto que el Derecho de la Unión no se aplica, en el estado actual de su evolución, a las normas que regulan la admisibilidad de las pruebas en el proceso penal, (…) la admisibilidad de las pruebas depende de que se respeten los requisitos y normas procesales que regulan la obtención de esas pruebas (…). Así pues, en este aspecto, *las normas nacionales aplicables en materia de práctica de la prueba deben respetar las exigencias derivadas de los derechos fundamentales garantizados por el Derecho de la Unión*". Es decir, no podrían utilizarse pruebas obtenidas a través de un régimen incompatible con los arts. 7, 8, 11 y 52 de la Carta Europea.

Pero el terremoto puede ser aún peor si, como quiera que el juez español es juez europeo y está obligado a salvaguardar la efectividad y primacía del Derecho de la UE, en cualquier

[26] Memorial anual 2013, pág. 739 y ss.

[27] En el mismo sentido, vid. RODRÍGUEZ LÁINZ, J. L. (2017). La definitiva defenestración…, op. cit.; TEJADA DE LA FUENTE, E. (2017). La conservación de datos informáticos con fines de investigación criminal; requisitos y condiciones para su incorporación al proceso penal. En: ZARAGOZA TEJADA, J. I. (coord.) *Investigación Tecnológica y Derechos Fundamentales. Comentarios a las modificaciones introducidas por la Ley 13/2015*. Cizur Menor: Thomson Reuters Aranzadi, p. 105; COLOMER HERNÁNDEZ, I. (2018). Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016. En RUDA GONZÁLEZ, A., JEREZ DELGADO, C. (coords.) *Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute*, Madrid: SEPIN editorial jurídica, p. 779.

momento —y subrayo esta incertidumbre e inseguridad jurídica en la que nos hallamos— un órgano judicial nacional decidiera declarar inaplicable la legislación española en materia de conservación de datos de comunicaciones electrónicas, en virtud del mandato establecido en el art. 4 bis 1 LOPJ por considerarla contraria al Derecho Europeo, a tenor de la evidente doctrina ratificada por el TJUE, y ello sin necesidad de plantear la correspondiente cuestión prejudicial ante el Tribunal de Luxemburgo, de acuerdo a lo preceptuado en el art. 267 TFUE, al amparo de la doctrina del TJUE sobre el "acto aclarado", en virtud de la cual el juez nacional español podría decidir no plantear la cuestión prejudicial si considera que la interpretación puede deducirse claramente de la jurisprudencia del Tribunal de Justicia y se impone de manera evidente, y como hemos indicado, la legislación española se asemeja sustancialmente a las legislaciones sueca y británica en materia de conservación de datos, que fueron declaradas incompatibles en virtud de la Sentencia *Tele2 Sverige y Watson* en 2016, y a la legislación belga sobre la misma materia, respecto a la cual las Conclusiones al Asunto C-520/18 del año 2020 también abogan por declarar su incompatibilidad con el Derecho de la Unión Europea.

Esta doctrina se encuentra ahora expresamente recogida en el art. 99 del Reglamento de Procedimiento del Tribunal de Justicia, según el cual "Cuando una cuestión prejudicial sea idéntica a otra sobre la que el Tribunal ya haya resuelto, cuando la respuesta a tal cuestión pueda deducirse claramente de la jurisprudencia o cuando la respuesta a la cuestión prejudicial no suscite ninguna duda razonable, el Tribunal podrá decidir en cualquier momento, a propuesta del Juez Ponente y tras oír al Abogado General, resolver mediante auto motivado". Y en la misma dirección, el apartado 6 de la versión actual —noviembre de 2019— de las Recomendaciones del TJUE a los órganos jurisdiccionales nacionales, relativas al planteamiento de cuestiones prejudiciales (2019/C 380/01) reitera que "Cuando la cuestión surja en un asunto pendiente ante un órgano jurisdiccional cuyas decisiones no son susceptibles de ulterior recurso judicial de Derecho interno, dicho órgano está obligado, sin embargo, a someter una petición de decisión prejudicial al Tribunal de Justicia (véase el artículo 267 TFUE, párrafo tercero), *a menos que exista ya una jurisprudencia bien asentada en la materia o no quepa ninguna duda razonable sobre el modo correcto de interpretar la norma jurídica*".

No obstante, es muy improbable que esta situación llegue a producirse en nuestro país. Esa decisión del órgano judicial sería inmediatamente recurrida, y si llegara en casación ante el Tribunal Supremo, existen dos importantes motivos para considerar que éste no inaplicaría directamente la Ley 25/2007 sin antes plantear, en su caso, una cuestión prejudicial ante el TJUE o una cuestión de inconstitucionalidad ante el TC.

El primero de esos motivos es de carácter exógeno: tras la STC 37/2019, de 26 de marzo, nuestro Tribunal Constitucional ha venido a exigir el necesario planteamiento de una cuestión de inconstitucionalidad ante el mismo, o en su caso, una cuestión prejudicial ante el TJUE, como "una garantía comprendida en el derecho al proceso debido frente a inaplicaciones judiciales arbitrarias o insuficientemente fundadas de la ley española basadas en una pretendida inconstitucionalidad de la misma o utilizando como excusa la primacía del Derecho comunitario".

El segundo argumento es endógeno: tras la STJUE de 8 de abril de 2014, el propio Tribunal Supremo siguió defendiendo a capa y espada que la declaración de nulidad de la Directiva 2006/24/CE no suponía la automática invalidez de la Ley que la traspone al derecho interno, aferrándose a aquello que más diferenciaba al régimen español de lo decretado con carácter de norma de mínimos por la Directiva de 2006: nuestro sistema imponía en todo caso un control judicial previo a la cesión de los datos; no cabía su empleo para la investigación de delitos no graves; y el legislador español había impuesto específicas medidas de seguridad en el tratamiento de la información[28]. Incluso después de la STJUE de 21 de diciembre de 2016, el Tribunal Supremo ha mantenido su postura defensiva y pivotante en torno a la exigencia de autorización judicial para la cesión de cualquier dato a los agentes facultados, lo que significa, en palabras del Alto Tribunal, que nuestro régimen "otorga la misma protección a derechos que no tienen la misma naturaleza y por ello idéntico nivel de tutela, como son los proclamados en el artículo 18.3, injerencia en el contenido de las conversaciones telefónicas, y la cesión de datos electrónicos de tráfico o asociados" y que la decisión judicial, "como quiera que deberá ser ajustada al principio de proporcionalidad establecido expresamente en nuestra ley procesal (artículo 588 bis a) 5 LECrim) (…) en principio no parece incompatible con la exigencia de una

[28] Vid., entre otras, las SSTS (Sala de lo Penal) núm. 470/2015, de 7 de julio, y 768/2015, de 23 de noviembre.

normativa nacional que no admita la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica[29]".

4. «MUERTE EN VENECIA»: LA APREMIANTE REFORMA DE LA LEGISLACIÓN ESPAÑOLA

La obra de Thomas MANN que sirve de título a este apartado está ambientada en una Venecia decadente sobre la que se cierne la epidemia del cólera, por más que las autoridades traten de ocultar el problema. De igual modo, sobre la normativa española en materia de conservación de datos de comunicaciones electrónicas se ciernen oscuros nubarrones que sólo podrán ser despejados con una exigente reforma en su propia raíz (la conservación). Otro símil con la obra de MANN para explicar nuestro estudio podría hacerse con respecto a su protagonista: *Aschenbach* renuncia a abandonar la ciudad, a pesar del peligro que corre, para no alejarse del joven *Tadzio*, y de igual modo, nuestros tribunales no desean desprenderse del preciado recurso que constituye ese "granero" de información sumamente eficaz en las investigaciones criminales, a pesar de que el mismo tiene los días contados por resultar desproporcionado e indiscriminado.

En nuestra opinión, la óptica utilizada por nuestro Tribunal Supremo para sostener la validez del sistema español de conservación de los datos generados con motivos de comunicaciones electrónicas y su uso en el proceso penal se encuentra desenfocada. Toda su atención se centra en señalar como «factor clave» el acceso a tales datos, el cual es cierto que ahora se encuentra sometido a una decisión judicial debidamente motivada y ponderada en función de la gravedad de los hechos, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes, la necesidad de la medida y la relevancia del resultado perseguido con la restricción del derecho, criterios todos ellos incorporados en virtud de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim, pero pasa de puntillas por el verdadero *pecado original* de nuestro ordenamiento jurídico: el desproporcionado régimen de conservación contenido en la Ley 25/2007.

El Tribunal Supremo guarda silencio sobre una realidad incontestable: el TJUE ha dejado meridianamente claro que las regulaciones nacionales no sólo deben contener específicas garantías que impidan un acceso automático o generalizado, sino también un específico régimen legal de «conservación selectiva», con criterios claros y objetivos, limitada y diferenciada en determinadas categorías de datos, absolutamente imprescindibles para prevenir y controlar eficazmente la delincuencia y para salvaguardar la seguridad nacional, durante un período determinado y diferenciado en función de cada categoría. Como señalan las Conclusiones de enero de 2020, la conservación y el acceso a los datos constituyen dos tipos distintos de interferencia que deben justificarse por separado, mediante un examen específico a la luz del objetivo perseguido, no pudiendo justificarse un sistema nacional que prevea el almacenamiento generalizado e indiferenciado de datos a cambio de instaurar requisitos rigurosos, materiales y procesales, para el acceso a dichos datos[30]. Dicho en otros términos, las lentes con las que los tribunales deben examinar la injerencia sobre los derechos fundamentales afectados en este ámbito no pueden ser monofocales, como sucedía en materia de interceptación de comunicaciones, sino bifocales (una «conservación selectiva» y un «acceso limitado»), sin que puedan contrarrestar una conservación extendida o indiscriminada a cambio de mayores controles y exigencias a la hora de ponderar la manera de acceder a los mismos.

Por ello, no es admisible importar a esta materia la construcción jurisprudencial, articulada a partir de la célebre STC 49/1999 en torno a la insuficiencia legal de la anterior redacción del art. 579 LECrim, según la cual la insuficiente adecuación del ordenamiento no implicaba por sí misma necesariamente la ilegitimidad constitucional de la actuación de los

[29] STS núm. 400/2017, de 1 de junio. En el mismo sentido, véase la STS núm. 723/2018, de 23 de enero de 2019.

[30] Aptdos. 73 y ss. de las Conclusiones al Asunto C-520/18. Tal y como gráficamente señala el Abogado General: "no comparto el argumento crítico que propugna el binomio «conservación más extendida a cambio de acceso más restringido»".

órganos jurisdiccionales, siempre que éstos hubieran actuado en el caso concreto respetando las exigencias dimanantes del principio de proporcionalidad.

La STC 184/2003, de 23 de octubre, dejó sentados tres parámetros para validar dicha labor jurisprudencial complementadora.

En primer lugar, afirmó: "si, pese a la inexistencia de una ley que satisficiera las genéricas exigencias constitucionales de seguridad jurídica, los órganos judiciales, a los que el art. 18.3 de la Constitución se remite, hubieran actuado en el marco de la investigación de una infracción grave, para la que de modo patente hubiera sido necesaria, adecuada y proporcionada la intervención telefónica y la hubiesen acordado respecto de personas presuntamente implicadas en el mismo, respetando, además, las exigencias constitucionales dimanantes del principio de proporcionalidad, no cabría entender que el Juez hubiese vulnerado, por la sola ausencia de dicha ley, el derecho al secreto de las comunicaciones telefónicas".

En segundo lugar, especificó: el anterior régimen del art. 579 LECrim "no es contrario a la Constitución por lo que dice, sino por lo que deja de decir —*un precepto con un núcleo o contenido constitucionalmente válido, pero insuficiente*, decía—. Ni siquiera hipotéticamente a través de una Sentencia interpretativa podría este Tribunal colmar todos los vacíos con la necesaria precisión por cuanto por medio de una interpretación no podría resolver en abstracto más de lo que de manera concreta haya ido estableciendo".

Y en tercer lugar, reclamó: "la intervención del legislador es necesaria para producir una regulación ajustada a las exigencias de la Constitución. (…) no es tarea de este Tribunal definir positivamente cuáles sean los posibles modos de ajuste constitucional, siquiera sea provisionalmente, hasta que la necesaria intervención del legislador se produzca".

Tales parámetros no resultan extrapolables al actual régimen español de conservación y acceso a los datos de comunicaciones electrónicas por los siguientes motivos.

En primer lugar, porque nuestro régimen de conservación indiscriminada de datos de comunicaciones electrónicas no debe considerarse insuficiente, vago o impreciso, como sucedía con el antiguo art. 579 LECrim, sino manifiestamente desproporcionado. Su contenido no es "constitucionalmente válido, pero insuficiente", sino generador *per se* de una injerencia desproporcionada en los Derechos Fundamentales a la vida privada y a la protección de los datos personales tal y como los mismos han sido interpretados por el TJUE, cuya jurisprudencia debe inspirar la labor interpretativa de los Tribunales nacionales (art. 10.2 CE). La afectación de los Derechos Fundamentales a la vida privada, la inviolabilidad de las comunicaciones y la protección de los datos personales no se produce únicamente cuando el órgano judicial pondera la necesidad de acceder a los datos conservados, lo cual sí sería jurisprudencialmente limitable, sino con la propia conservación en virtud de una imposición legal excesiva. En tal caso, se está aplicando una normativa nacional que afecta al cumplimiento y efectividad de los derechos que se derivan del Derecho de la Unión, de modo que tendría que respetar y ser compatible con el Derecho Europeo[31], y nuestra ley de conservación no lo es.

En segundo lugar, porque esa labor ponderadora de los órganos jurisdiccionales para suplir la insuficiencia de la ley y respetar las exigencias constitucionales dimanantes del principio de proporcionalidad ya ha sido objeto de *interpositio legislatoris* (L.O. 13/2015) para, precisamente, ofrecer al juez los principios rectores que deben presidir la adopción de la correspondiente y más idónea diligencia tecnológica de investigación. Pero ese nuevo régimen legal ahora contenido en la LECrim complementa el sistema de cesión de datos de tráfico, pero no el sistema de conservación.

Y en tercer lugar, porque la jurisprudencia podrá delimitar y restringir la afectación del Derecho Fundamental afectado (arts. 18,1 y 18.4, y en su caso, art. 18.3 CE) cuando se trata de acceder a los datos conservados, de acuerdo con las nociones de especialidad, idoneidad, excepcionalidad, necesidad y demás requisitos previstos en el nuevo régimen contenido en los arts. 588 bis LECrim y siguientes, pero no podrá perfilar los límites legales de tal conservación.

---

[31] Sobre este punto, vid. la STJUE *Akerberg Fransson*, de 26 de febrero de 2013, asunto C-617/10. Como comentario a la misma, vid. DE HOYOS SANCHO, M. (2018). Los efectos expansivos del derecho de la unión Europea sobre las garantías en el proceso penal. En JIMÉNEZ CONDE, F. (dir.). *Adaptación del derecho procesal español a la normativa europea y a su interpretación por los tribunales*. Valencia: Tirant lo Blanch, p. 46.

Es decir, el auto judicial habilitante de la segunda injerencia (acceso) sí que podrá limitar la intromisión concretando el alcance o extensión de la medida —cualidad y naturaleza de la información solicitada, periodo de información a remitir, número de sujetos y de terminales sobre los que recae la solicitud policial, etc.— pues la investigación penal de un delito grave no tiene por qué conllevar, siempre y en todo caso, la máxima intensidad en el sacrificio de los derechos fundamentales que convergen en el momento de cualquier comunicación telefónica o telemática, que es lo que precisamente acontece en España, y no con origen en una resolución judicial motivada, sino en un deber legal impuesto con carácter genérico a las operadoras de telefonía[32]. No es que el auto judicial pueda llegar a ser, como dice MARCHENA GÓMEZ, una suerte de "red de arrastre digital" no conforme con la debida motivación y ponderación de los intereses en juego, sino que el propio régimen legal de conservación de datos es un tipo de pesca proscrita por el Derecho de la Unión Europea. Esa labor corresponde exclusivamente al legislador, que debe adecuar la Ley 25/2007 al Derecho de la Unión Europea y a los Derechos Fundamentales recogidos en la Carta Europea tal y como han sido interpretados por el TJUE.

En contra de la doctrina jurisprudencial de nuestro país a propósito de la anterior dicción del art. 579 LECrim, ya advertimos en su momento que esa continua adaptación judicial de una raquítica legislación a las constantes innovaciones tecnológicas corría el riesgo de no superar, en algún momento, las exigencias de legalidad, claridad y previsibilidad establecidas por el TEDH y el tiempo nos dio la razón[33]: el Tribunal Constitucional, en su STC 145/2014, de 22 de septiembre, puso *pies en pared* ante la tendencia del Tribunal Supremo de interpretar hiperbólicamente el art. 579 LECrim, exigiendo una habilitación legal con calidad. Dicha Sentencia constituyó el aldabonazo definitivo para que nuestro legislador reconvirtiera a marchas forzadas algunos apartados de un futurible Código Procesal Penal en un texto legislativo acorde con las exigencias del TEDH. Esperemos no tener que lamentar una adecuación tardía del régimen español de conservación de datos a las exigencias del TJUE.

En conclusión, la defensa numantina de la legislación española por parte del Tribunal Supremo y de reputados miembros de la carrera judicial y fiscal resulta elogiable. Más, si cabe, si la comparamos con la tradicional parálisis del legislador español en materia procesal penal. Que el Poder Legislativo de nuestro país no reformase la Ley 25/2007 a través de la Ley General de Telecomunicaciones de 2014 es entendible, dado el escaso lapso temporal transcurrido entre el dictado de la STJUE *Digital Rights* (8 de abril) y la publicación de la Ley 9/2014 en el BOE (11 de mayo). Que no lo hiciera a través de la Ley Orgánica 13/2015 (5 de octubre de 2015) sí merece cierto reproche. Pero que no haya iniciado, tan siquiera, alguna propuesta legislativa a partir de las SSTJUE de 21 de diciembre de 2016 y 2 de octubre de 2018 es, sencillamente, indignante[34].

4.1. La debilidad: la inexistencia de criterios legales objetivos para una «conservación selectiva» de datos

Sabedor de la necesidad y utilidad de que los Estados puedan fijar legalmente obligaciones de conservación de datos de comunicaciones electrónicas con el fin de salvaguardar la seguridad nacional y luchar eficazmente contra la delincuencia, el TJUE no se

[32] MARCHENA GÓMEZ, M. (2011). La vulneración de derechos fundamentales por ministerio de la Ley (a propósito del art. 33 de la Ley General de Telecomunicaciones), *Diario La Ley*, núm. 7572, de 18 de febrero. Véanse también sus votos particulares a las SSTS de 6 de octubre de 2011 y de 20 de enero de 2012.

[33] ORTIZ PRADILLO, J. C. (2017). desafíos legales de las diligencias de investigación tecnológica. En FUENTES SORIANO, O. (coord.). *EL PROCESO PENAL. Cuestiones fundamentales*. Valencia: Tirant lo Blanch, p. 306. Otros argumentos en los que basamos la necesidad de reformar la Ley 25/2007 se contienen en ORTIZ PRADILLO, J. C. (2013). *Problemas procesales…*, op. cit., pp. 218 y ss.

[34] En la misma línea, COLOMER HERNÁNDEZ, I. (2018). La cesión de datos de las comunicaciones electrónicas para su uso en investigaciones criminales: una problemática en ciernes. En JIMÉNEZ CONDE, F. (dir.). *Adaptación del derecho procesal español a la normativa europea y a su interpretación por los tribunales*. Valencia: Tirant lo Blanch, p. 99, también advierte que "la pasividad del poder ejecutivo, que no ha presentado ningún proyecto de ley (…) está incubando un grave problema cuyas consecuencias duando estalle pueden ser muy graves para todo el sistema criminal español".

opone a la implantación de regímenes nacionales de conservación de datos, siempre y cuando los mismos no conviertan en regla general una conservación genérica e indiscriminada, cuyo único límite lo constituye el factor temporal, tal y como ahora sucede. Debe tratarse de una «conservación selectiva», con criterios claros y objetivos, limitada y diferenciada en determinadas categorías de datos, absolutamente imprescindibles para prevenir y controlar eficazmente la delincuencia y para salvaguardar la seguridad nacional, así como limitada a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia.

Veamos con más detalle esos criterios que los Estados miembros deberán tener presentes a la hora de configurar sus regímenes nacionales.

4.1.1. Criterios subjetivos

Tal y como lo menciona el TJUE ("círculo de personas"), el criterio subjetivo resulta, sin duda, el más complejo de estipular legislativamente con carácter preventivo, pues la conservación de comunicaciones electrónicas para una futura investigación aún no iniciada "nos acerca más bien al campo, también legítimo, de la seguridad pública o seguridad nacional, de labores de inteligencia; donde las técnicas prospectivas ganan toda su razón de ser. Una retención/conservación de datos de futuro para una concreta investigación criminal es una técnica de investigación que poco o nada tiene que ver con las herramientas de conservación preventiva en las que estaba pensando el legislador comunitario al redactar el art. 15.1 de la Directiva[35]". Hasta el propio Abogado General advierte la dificultad de tal empresa, pues "La elección de esos grupos podría abocar, además, a instaurar un régimen de sospecha general sobre algunos segmentos de la población y catalogarse de discriminatoria, en función del algoritmo empleado[36]".

La exclusión de ciertos sujetos resulta más sencilla —por ejemplo, en virtud de ciertas inmunidades o prerrogativas como el deber de secreto profesional—, pero la selección de los sujetos afectados será compleja, salvo que el criterio subjetivo se delimite desde otras perspectivas. Así por ejemplo, y en vez de poner el acento en el sujeto activo de la comunicación, planteamos aquí la conveniencia de atender al aspecto pasivo de la comunicación y determinar la necesaria conservación de las comunicaciones o conexiones recibidas por determinadas personas, organismos o entidades. Y también defendemos la ventaja que supondría acudir a otros criterios complementadores, como por ejemplo, poner el foco en que se trate de usuarios de un concreto tipo de comunicación o de un concreto modelo de dispositivo.

Nuestra legislación ya cuenta con antecedentes a la hora de exigir el registro de usuarios de determinadas comunicaciones o determinados instrumentos. Como referentes, la Disposición adicional única de la Ley 25/2007 ya previó la obligatoriedad de llevar un libro-registro por parte de los operadores de servicios de telefonía móvil que comercialicen *servicios con sistema de activación mediante la modalidad de tarjetas de prepago*, en el que debía constar la identidad de los clientes. En la misma línea, el art. 25 de la Ley Orgánica 4/2015, de 30 de marzo, de Seguridad Ciudadana amplió la llevanza de tales libros-registros a otras actividades entre las que incluyó el *acceso comercial a servicios telefónicos o telemáticos de uso público mediante establecimientos abiertos al público*, (lo cual permitiría sustentar la legitimidad de la conservación de las comunicaciones efectuadas desde dichos establecimientos). Y en materia de uso de aeronaves no tripuladas —los denominados *Drones*— El R.D. 1036/2017, de 15 de diciembre, exige a los operadores de determinados aparatos, inscribir en el Registro de Matrícula de Aeronaves Civiles los datos identificativos de la aeronave, *así como el nombre del operador y los datos necesarios para ponerse en contacto con él* (arts. 8 y 9) y llevar un registro de los datos relativos a los vuelos realizados y el tiempo de vuelo, entre otros aspectos (art. 16.2.a). Ello se complementa con el mandato establecido en el Reglamento de Ejecución (UE) 2019/947 de la Comisión, de 24 de mayo de 2019, de registrar los datos identificativos de los operadores de las aeronaves no tripuladas cuando las mismas *estén equipadas con un sensor capaz de capturar datos personales*, salvo que sea conforme con la Directiva 2009/48/CE (art. 14.5).

---

[35] RODRÍGUEZ LÁINZ, J. L. (2017). La definitiva defenestración…, op. cit., p. 13.
[36] Apartado 88 de las conclusiones al Asunto C-520/18.

Entendemos que estos criterios (sujeto receptor de la comunicación, usuario de un determinado sistema de comunicación o dispositivo) resultan igualmente enfocados al aspecto subjetivo, pero más fáciles de convertir en pautas legales de definición de la información a conservar.

4.1.2. Criterios geográficos

El criterio espacial puede llegar a utilizarse como criterio adicional, y en ocasiones sustitutivo del subjetivo, cuando el ámbito geográfico pueda ser en sí mismo un factor determinante a la hora de definir el riesgo que se pretende prevenir, como por ejemplo, situaciones de grandes aglomeraciones humanas o acontecimientos de índole política o económica de especial relevancia, en los que la prevención de atentados terroristas debiera partir de criterios exclusivamente espaciales, o la delimitación de espacios o ámbitos territoriales donde se desenvuelven con asiduidad actividades delictivas generalmente relacionadas con la actuación de grupos organizados[37].

En efecto, la celebración de determinados eventos multitudinarios susceptibles de ser delimitados temporal y espacialmente (por ej., una cumbre de jefes de Estado, una feria internacional o una final deportiva a la que asistirán miles de personas) podrían servir de base para justificar la recopilación genérica de datos sobre comunicaciones y ubicaciones que tengan lugar en dicho ámbito geográfico y en los periodos inmediatamente anteriores y posteriores a dichas celebraciones —y con el deber de eliminación automática tras un determinado periodo de tiempo—, para prevenir la comisión de atentados terroristas e identificar a sus integrantes o partícipes. La segunda opción (delimitación de zonas con asiduidad delictiva) se antoja más difícil de precisar, a riesgo de caer en la estigmatización de ciertos barrios y lugares, y la conservación preventiva de datos derivados de comunicaciones electrónicas tendría una eficacia muy limitada. Que en una zona sea frecuente un determinado tipo de delincuencia en determinadas franjas horarias (robos, tráfico de drogas,…) puede justificar la videovigilancia de la misma (joyerías, zonas comerciales o de ocio nocturno, lugares de desembargo de alijos o de tráfico de estupefacientes…), y quizás la conservación preventiva de los datos de localización de los dispositivos que hayan utilizado las antenas BTS del lugar durante un concreto periodo de tiempo, pero esto apenas servirá para luchar contra un concreto tipo de delincuencia. Otra delincuencia sumamente grave y heterogénea, como es la ciberdelincuencia, resulta difícilmente acotable espacialmente hablando.

No obstante, el bagaje y las previsiones legales en materia de videovigilancia de lugares públicos sí nos podría servir de referencia a la hora de justificar geográficamente la necesidad y proporcionalidad de una conservación preventiva de determinados datos referidos a comunicaciones electrónicas. Al igual que se estima necesario efectuar un control preventivo de ciertos lugares, edificios e infraestructuras, puede tener cabida y justificarse la necesidad de conservar preventivamente determinados datos de conexiones y comunicaciones electrónicas que tengan lugar, origen o destino de esos lugares e infraestructuras[38]. Para ello, el régimen legal podría someter dicha justificación a informes previos de determinados organismos o comisiones sectoriales, como sucede, por ejemplo, cuando se trata de justificar un peligro concreto para delimitar el uso de videocámaras móviles en lugares y momentos puntuales. Y dicho régimen debería igualmente regirse por la regla general de eliminación automática de lo retenido tras un determinado periodo de tiempo (nunca tan amplio como los actuales 12 meses), salvo que se apreciara la comisión de un delito que motivara su petición a las operadoras.

4.1.3. Criterios materiales o teleológicos

La delimitación por categorías o tipologías de datos en función del fin a alcanzar o de su mayor o menor afectación a la privacidad de las personas, también debe ser un criterio legal

[37] RODRÍGUEZ LÁINZ, J. L. (2017). Ult. op. et loc. cit.

[38] Para LÓPEZ BARAJAS, I. (2009). El deber de conservación de datos en la unión europea y sus límites, *Revista de Derecho de la Unión Europea*, nº 16 - 1er semestre, p. 195 y ss., en determinados supuestos como la videovigilancia en los bancos o el uso de cacheos y registros en los aeropuertos, la falta de indicios concretos se compensa por las especiales circunstancias que concurren en el lugar que hacen razonable la intervención o control.

expreso. En los apartados 92 y siguientes del Asunto C-520/18, el AG Campos Sánchez-Bordona propone, entre otros, diferenciar entre datos de abonado, datos de tráfico y asociados a las comunicaciones, con sus múltiples subcategorías, o datos de contenido; la pseudonimización de los datos; la implantación de períodos de conservación limitados; la exclusión de algunas categorías de proveedores de servicios de comunicaciones electrónicas; las autorizaciones de almacenamiento renovables; la obligación de conservar los datos almacenados dentro de la Unión o el control sistemático y regular por parte de una autoridad administrativa independiente de las garantías ofrecidas por los prestadores de servicios de comunicaciones electrónicas contra el uso indebido de los datos.

4.1.4. Criterios temporales

Como quiera que el TJUE ha advertido que la injerencia en la intimidad de los ciudadanos no sólo se produce cuando las autoridades acceden a esos datos, sino desde el mismo momento en que los mismos son retenidos, clasificados, almacenados y, en su caso, cruzados con otros segmentos de información, la «conservación selectiva» también deberá atender a limitaciones temporales en función del objetivo perseguido o de las tipología del dato conservado.

La dimensión temporal de la medida constituye un factor esencial a la hora de determinar el grado de afectación de los derechos en juego. A mayores periodos de conservación, mayor riesgo de interferir en los derechos fundamentales de las personas, pues si lo conservado es un aspecto puntual o periodo corto, estaremos ante un «fotografía» ilustrativa de lo acontecido en un momento preciso del pasado (una comunicación), mientras que si lo conservado atiende a un periodo mayor, estaremos ante una serie de «fotogramas» capaces de reproducir un comportamiento, una costumbre, o un estilo de vida ilustrativo de la personalidad del sujeto investigado. No es lo mismo conservar los datos identificativos de los terminales conectados a una concreta antena BTS de telefonía, que conservar la ruta o interacciones de esos terminales durante sus desplazamientos, y en su caso, durante sus comunicaciones. La conservación sistemática de los datos de geolocalización del teléfono móvil de una persona, por ejemplo, permite extraer aspectos sumamente íntimos de aquélla[39] (sus preferencias religiosas —frecuenta una mezquita—, sexuales —frecuenta un bar gay, club de alterne, domicilio del amante—, políticas —asiste a un determinado mitin o manifestación—, su salud —prácticas de aborto, tratamiento de VIH—, vida personal y familiar, rutas —donde y a qué hora puede ser secuestrado—) que deberán ser objeto de especial protección y de excepcional y limitada conservación.

El art. 588 bis a) LECrim especifica certeramente que el principio de idoneidad sirve para definir "el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad". Es decir, la idoneidad debe siempre examinarse desde un punto de vista cualitativo —tipología de la medida de investigación— y cuantitativo —duración de la misma—. Sucede, sin embargo, que esta regla no es usada para delimitar el alcance temporal de la conservación de los datos, que se rige por la legislación sustantiva; un plazo común de 12 meses, con independencia del tipo de dato, autor o receptor de la comunicación o medio de comunicación empleado.

Por tanto, el futuro régimen legal español deberá huir de un periodo de conservación único y tan extenso como prevé el actual art. 5.1 de la Ley 25/2007 (nada menos que 12 meses, mientras que el TJUE está anulando leyes nacionales que imponen un periodo máximo de 6 meses) y establecer una oportuna graduación de los periodos máximos de conservación, por ejemplo, en atención a la naturaleza del dato conservado y su capacidad de revelar aspectos más o menos precisos de su personalidad.

El camino lo marcó la STJUE *Ministerio Fiscal* al considerar una «injerencia no grave» la obtención de los datos de titularidad de las tarjetas SIM activadas con el teléfono móvil sustraído, sin que los mismos fueran objeto de cotejo "con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización". Es decir, la conservación de los datos de usuarios y abonados podrá tener una duración mayor que los datos de tráfico de comunicaciones efectuadas o intentadas (ej., la fecha, hora y duración de una comunicación o el tipo de comunicación —transmisión de voz, buzón vocal, conferencia, datos,…—), y éstos, a su vez,

[39] VELASCO NÚÑEZ, E. (2014). Tecnovigilancia, geolocalización y datos: aspectos procesales penales", *Diario La Ley*, núm. 8338, de 23 de junio de 2014.

podrán ser objeto de una conservación mayor que los datos de localización (la etiqueta de localización al inicio de la comunicación o las celdas de las antenas BTS que entren en juego durante una comunicación).

En resumen, la facultad establecida en el propio art. 5.1 de la Ley 25/2007, que permite ampliar o reducir el plazo de conservación "para determinados datos o una categoría de datos", pero no tomando en consideración el coste del almacenamiento y conservación de los datos, sino *el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave*, deberá ser una realidad expresamente delimitada y desarrollada en la Ley y no una opción reglamentaria aún sin desplegar.

4.2. La fortaleza: el régimen de la LECrim como canon interpretativo para un «acceso limitado» a los datos

Si aunamos la jurisprudencia sentada en las Sentencias *Digital Rights, Tele2 Sverige y Watson* y *Ministerio Fiscal* y las Conclusiones de enero de 2020, podemos anticipar los requisitos que deberá cumplir el régimen nacional regulador de un «acceso limitado» para ser considerado compatible con el Derecho de la Unión.

4.2.1. Requisitos generales

Por un lado, deberá contener un régimen general sujeto a tres principios rectores: a) el acceso deberá someterse a un control previo (admitiéndose un control *a posteriori* en casos de urgencia debidamente justificados) por parte de un órgano jurisdiccional o de una entidad administrativa independiente que examine la solicitud, en el marco de procedimientos de prevención, descubrimiento o acciones penales; b) las autoridades nacionales competentes a las que se conceda el acceso a los datos conservados deberán informar de ello a las personas afectadas, en el marco de los procedimientos nacionales aplicables, siempre que esa comunicación no pueda comprometer las investigaciones que llevan a cabo esas autoridades; y c) dicho acceso deberá estar revestido de expresas normas en materia de seguridad y protección de los datos que obran en poder de los proveedores de servicios de comunicaciones electrónicas, a fin de evitar el uso indebido y el acceso ilícito a los datos.

En nuestra opinión, el régimen español ya se adecúa en gran medida a estos tres pilares, si bien deberá modificarse para incorporar explícitamente la regla general de informar a las personas afectadas por la injerencia. Cuando se promulgó la Ley de 2007, ya cuestionamos que, tratándose de una ley ordinaria, contuviera en su art. 9 «excepciones» a los derechos de acceso y cancelación previstos en la LOPD, pues tales derechos deben ser considerados parte del contenido esencial del Derecho Fundamental al *Habeas Data*[40]. Para ello, la regla prevista en el art. 588 ter i) 3. LECrim, que dispone la notificación de la injerencia —interceptación de comunicaciones— "a las personas intervinientes en las comunicaciones interceptadas" con determinadas salvaguardas, debería ser extrapolada igualmente a la diligencia prevista en la letra j) del referido artículo —acceso a datos obrantes en archivos automatizados de los prestadores de servicios—.

4.2.2. Requisitos especiales

[40] Según la STC 292/2000, de 30 de noviembre (F.J. 6º), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, *el derecho a saber y ser informado sobre el destino y uso de esos datos* y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, F. J. 7). Esa insuficiencia jerárquica también fue expresamente evidenciada por el Tribunal Supremo (STS núm. 249/2008, de 20 de mayo).

Por otro lado, deberá contener un régimen especial sobre la proporcionalidad de la injerencia (juicio abstracto de la ley), graduada de conformidad con los siguientes criterios o parámetros de ponderación.

4.2.2.1. En función de la tipología o categoría del dato solicitado

Como pauta inicial, admitimos que el acceso a datos de titularidad o de identificación del usuario o abonado —*subscriber data*— pueda reputarse como una injerencia no grave, mientras que el acceso a datos asociados o generados con motivo de una comunicación, como sucede con los datos de tráfico —*traffic data*— y de localización —*location data*— deberían considerarse injerencias graves. De hecho, ese ha sido tradicionalmente el criterio utilizado por la jurisprudencia española, que siempre ha examinado si el Derecho Fundamental afectado era la intimidad (art. 18.1 CE), la protección de los datos personales (art. 18.4 CE) o el secreto de las comunicaciones (18.3 CE) precisamente para eximir del control judicial previo aquellas injerencias en la intimidad que no afectaran a procesos comunicativos, efectuando además una apreciable "jibarización[41]" de lo que debía considerarse como «comunicación» a los efectos de reclamar la aplicación de las garantías derivadas del art. 18.3 CE, a través de un progresivo encaje de las comunicaciones ya consumadas en el ámbito de la privacidad y un abandono de esa perpetuación de la protección formal del art. 18.3 CE a comunicaciones ya consumadas.

Por ello, y aunque la jurisprudencia ha terminado por reconocer la existencia de un «entorno virtual[42]» del individuo que exige una visión unitaria —y sujeta como regla general a la exclusividad judicial— que supere ese tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en las nuevas formas de interacción electrónica, no vemos inconveniente en que se asuma esa inicial diferenciación. Y así, frente a la imprecisa cláusula del art. 1.2 de la Ley 25/2007, los arts. 588 ter j) y m) LECrim sí que diferencian entre datos "vinculados a procesos de comunicación" y datos "de titularidad de un número de teléfono o de cualquier otro medio de comunicación[43]".

Pero tal diferenciación inicial no debe dar lugar a automatismos según se vea o no afectado un proceso comunicativo, sino que también deberá tenerse en cuenta si la tipología del dato a obtener permite "conclusiones precisas acerca de la vida privada de la persona afectada", incluso más que con el acceso al contenido de las comunicaciones. Como venimos sosteniendo hace tiempo, el desarrollo tecnológico ha obligado a abandonar la "terminología *Malone*" que diferenciaba entre «contenido» propiamente dicho y «datos externos» de las comunicaciones y no puede considerarse, sin más, que el conocimiento y uso de los "datos de tráfico" de aquéllas

[41] Sobre dicha tendencia, vid. ORTIZ PRADILLO, J. C. (2017). Comunicaciones, Tecnología y Proceso Penal: viejos delitos, nuevas necesidades. En ASENCIO MELLADO, J. M. (dir.) *Justicia penal y nuevas formas de delincuencia*. Valencia: Tirant lo Blanch, p. 29 y ss.

[42] STS núm. 342/2013, de 17 de abril y STC 115/2013, de 9 de mayo.

[43] Para OROMÍ I VALL-LLOVERA (op. cit., p. 8) "existe una contradicción evidente entre la doctrina del TJUE, que considera este tipo de acceso a datos personales como una injerencia no grave de los derechos fundamentales a la protección de datos de carácter personal y a la vida privada y familiar, y el sistema español, lo que hace surgir la duda sobre si el artículo 588 ter m LECrim es conforme al derecho de la Unión Europea. A mi juicio, pese a que la injerencia no es grave, sigue siendo una vulneración de los derechos fundamentales de los ciudadanos que debe precisar de autorización judicial". Mi opinión es la contraria, y coincide con la recogida en el *Dictamen nº 1/19 de la Unidad de Criminalidad Informática de la Fiscalía General del Estado acerca del alcance de la reclamación de datos de identificación de titulares, terminales y/o dispositivos de conectividad prevista en el nuevo artículo 588 ter m de la Ley de Enjuiciamiento Criminal*, según la cual cabe solicitar a las operadoras, sin una necesaria autorización judicial previa, la identidad de quien sea el titular de un número de teléfono o de cualquier otro medio de comunicación, así como también, y en sentido inverso a la averiguación de los números de teléfono y/o datos identificativos de cualquier otro medio de comunicación (por ej., los códigos IMSI e IMEI), siempre que la solicitud/facilitación de los mismos se haga como dato independiente y aislado o desvinculado de cualquier información sobre los procesos comunicativos en que dichas numeraciones hayan podido ser utilizadas.

afecta en menor medida (supone una «injerencia de menor intensidad[44]») que el conocimiento del contenido. La recopilación sistemática y cruce inteligente de dichos datos externos almacenados puede suponer una injerencia en el Derecho Fundamental al *Habeas Data* del art. 18.4 CE mucho mayor que el simple acceso al contenido de una conversación[45]. Así lo reconoció el propio TJUE en la Sentencia *Tele2 Sverige* (aptdo. 99), al advertir que los datos de tráfico y localización proporcionan "información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones". Y así lo ha reconocido también el propio Tribunal Supremo (STS 740/2017, de 16 de noviembre), para quien "Las comunicaciones telefónicas a través de la telefonía móvil y las telemáticas por medio de Internet nos sitúan en un rupturista escenario en el que tanta importancia puede llegar a tener para la investigación el conocimiento de las conversaciones interceptadas, como el de los datos electrónicos asociados a aquéllas".

4.2.2.2. En función de la cantidad de datos solicitados o del número de peticiones referidas a un mismo sujeto

En efecto, a mayor cantidad de información solicitada a las empresas y demás sujetos colaboradores, mayor capacidad de las autoridades investigadoras para efectuar análisis inteligentes y trazar los temidos "perfiles integrales de la personalidad", y como quiera que el actual desarrollo tecnológico de las comunicaciones ha dado lugar a nuevos formatos y nuevas tipologías de datos de muy diversa índole, la ponderación a realizar sobre el alcance de la medida deberá ser mayor. Debemos recordar que "intervenir un teléfono no es lo mismo que intervenir un teléfono más todos los datos de identidad, SMS, listado de llamadas, correos electrónicos, ubicación geográfica, etc., que automáticamente facilita el sistema y obligatoriamente ha de ceder el operador. En este aspecto, la nueva tecnología permite una inmisión en la intimidad (en sentido amplio) mucho más potente que la que suponía el clásico «pinchazo», lo que no puede quedar extramuros de la exigencia de ponderación que se imponía al juez en el marco analógico[46]".

4.2.2.3. En función de la extensión del periodo de tiempo a que se refiera el acceso

Lo que permite apreciar la gravedad de la injerencia es "la conjunción entre la naturaleza de los datos en cuestión y la duración del período al que se refiere el acceso", en el sentido de que un acceso a datos de un período suficientemente largo permite revelar con suficiente precisión los rasgos principales de la vida de una persona[47]. No en vano, uno de los aspectos valorados en la Sentencia *Ministerio Fiscal* fue precisamente la duración del período a que se refería el acceso (12 días) para catalogar la injerencia como "no grave".

Esto nos recuerda a la doctrina sentada por la Corte Suprema de los EE.UU en materia de recolección y acceso a los datos de localización basados en la tecnología GPS: En el caso *Knotts* (1983) se legitimó la instalación de una baliza GPS sin necesidad de una decisión judicial previa porque el rastreo se limitó a unas horas, mientras que en el caso *Jones* (2012) se consideró que sí había habido una afectación a la Cuarta Enmienda con motivo de la instalación de un dispositivo GPS en un vehículo, no sólo por el desarrollo de la tecnología y del instrumento utilizado, sino también por el grado cuantitativo de la injerencia sobre la privacidad de los individuos, pues la policía controló los movimientos del vehículo del sospechoso las 24 horas del

---

[44] Vid. SSTC 123/2002 y 26/2006: *aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las «escuchas telefónicas», siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad*.

[45] ORTIZ PRADILLO, J. C. (2010). Tecnología versus Proporcionalidad…, op. cit., pp. 80-94.

[46] CRESPO BARQUERO, P. (2010). Intervenciones judiciales en materia de comunicaciones telefónicas e Internet, *Cuadernos Penales José María Lidón*, núm.7/2010, p. 92. En el mismo sentido, vid. MARCHENA GÓMEZ, M. (2011). La vulneración de derechos fundamentales…, op. cit.

[47] Vid. apartado 82 de las Conclusiones C-746/18.

día durante 28 días[48]. Y en el asunto *Carpenter* (2018), la Corte advierte que el seguimiento de los movimientos pasados de una persona a través del acceso a los datos de posicionamiento de su teléfono móvil conservados por las operadoras constituye una injerencia sobre la intimidad de las personas mucho mayor que con el monitoreo GPS, pues ofrece "una ventana a la vida privada reveladora, no sólo de sus concretos movimientos, sino también, y a través de ellos, sus vínculos familiares, políticos, profesionales, religiosos y sexuales" y otorga al gobierno "una vigilancia perfecta que le permite viajar atrás en el tiempo para rastrear el paradero de una persona".

Por tanto, el futuro régimen legal español no sólo deberá prever un sistema de periodos de conservación, que deberán ser graduales a la naturaleza del dato y a su utilidad para alcanzar los objetivos perseguidos, sino también unos criterios que sirvan de pauta para limitar y ponderar el periodo objeto de solicitud de acceso/cesión a las autoridades, tanto de datos históricos como de interceptación de datos generados en tiempo real, que deberán ser proporcionados a estos parámetros aquí expuestos.

En España, el acceso a datos interceptados en tiempo real puede tener una duración mayor que la del acceso a datos históricos almacenados. En ambos casos, los plazos manejados por la legislación española nos parecen excesivos, pero entendemos que los primeros puedan tener un mayor alcance (hasta 18 meses, para datos interceptados con motivo de una comunicación —588 ter g LECrim— o para datos de geolocalización del dispositivo instalado —588 quinquies c LECrim—) porque la injerencia se acuerda motivadamente por un órgano judicial en el seno de unas investigaciones concretas contra un sujeto presuntamente autor de unos hechos con relevancia penal, mientras que los segundos (hasta 12 meses, según el art. 5.1 de la Ley 25/2007) tienen su origen en una imposición legal que afecta a cualquier ciudadano.

Tras la reforma de la LECrim en 2015, el acceso a esos datos obtenidos en tiempo real sí cuenta al menos con pautas legales para que el órgano judicial gradúe el alcance temporal de la injerencia, mientras que el periodo de acceso a datos históricos se encuentra huérfano de una mínima calidad reguladora que ilustre al juez sobre cómo delimitar temporalmente tal injerencia, razón por la cual deberá ser objeto de reforma.

Así, a la hora de acordar la medida de investigación tecnológica correspondiente, el juez debe tener presente las siguientes directrices de carácter temporal: en primer lugar, el art. 588 bis a) LECrim le obliga a valorar la idoneidad de la medida atendiendo al ámbito objetivo y subjetivo "y la duración de la medida en virtud de su utilidad". En segundo lugar, la letra e) del apartado 3º del art. 588 bis c) LECrim le obliga a concretar la duración de la medida en la resolución judicial habilitante. Sucede, no obstante, que el art. 588 bis e) LECrim dispone que la duración de *las medidas reguladas en el presente capítulo* será "la que se especifique para cada una de ellas y no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos", y sin embargo, ningún parámetro temporal concreto se menciona en el art. 588 ter j) LECrim al regular la cesión de datos electrónicos conservados, a diferencia de lo que sucede con otras concretas medidas[49].

Por lo tanto, cuando la medida de investigación consista en requerir a las operadoras y demás sujetos o empresas que presten servicios en la Sociedad de la Información para que faciliten esos datos conservados "en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación", la solución debiera ser una de las siguientes: O bien se aboga por establecer legalmente unos criterios delimitativos del

[48] Un análisis a los criterios de ponderación utilizados por la Corte Suprema de los EE.UU. respecto de la incidencia de la tecnología en las actuaciones policiales puede verse en ORTIZ PRADILLO, J. C. (2013). El impacto de la tecnología en la investigación penal y en los derechos fundamentales. En: GONZÁLEZ-CUÉLLAR SERRANO, N. (dir.). *Problemas actuales de la justicia penal*. Madrid: Colex, pp. 317-341.

[49] La interceptación en tiempo real de datos (art. 588 ter g) está sujeta a un periodo inicial máximo de 3 meses, prorrogables hasta un máximo de 18 meses. Los mismos plazos se prevén para la utilización de dispositivos de localización y seguimiento (art. 588 quinquies c) también. Los registros remotos (art. 588 septies c) quedan reducidos a un plazo inicial máximo de un mes, prorrogable por iguales períodos hasta un máximo de 3 meses. Y el deber de conservación de datos informáticos (art. 588 octies II) se limita a un inicial plazo máximo de 90 días, prorrogable una sola vez por igual período hasta llegar a un máximo de 180 días.

alcance temporal del acceso (por ej., en función de la tipología del dato y en función de la gravedad del delito investigado), o bien se aboga por exigir del órgano judicial una manifestación expresa del alcance temporal de la medida, en virtud de una interpretación conjunta de las reglas contenidas en el art. 588 bis c. 3.e) LECrim y el 588 ter j.2 LECrim, en el siguiente sentido: El juez deberá concretar la duración de la medida en la resolución judicial habilitante, y si tal resolución obedeciera a una petición policial o del Ministerio Fiscal, como quiera que se exige precisar "la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión", el juez también debiera exigir al solicitante que justifique el marco temporal respecto del cual se precisan los datos.

4.2.2.4. En función de la gravedad del delito

Llegados a este punto, si bien se insiste por parte de los Abogados Generales del TJUE en que la noción de «delito grave» debe quedar a la apreciación de los Estados miembros según sus sistemas jurídicos nacionales, el Sr. Pitruzzella especifica que "la sanción aplicable no constituye el único criterio para determinar la gravedad de las infracciones (aptdo. 93). También es preciso tener en cuenta otros criterios como la naturaleza de las infracciones, el daño que causan a la sociedad, el menoscabo que provocan en los intereses jurídicos y los efectos generales que producen en el ordenamiento jurídico nacional, así como en los valores de una sociedad democrática, el contexto histórico, económico y social específico de cada Estado miembro o si los delitos han sido cometidos, bien de manera reiterada, bien contra colectivos vulnerables.

Este listado de criterios de ponderación propuesto por el Sr. Pitruzzella no sólo refuerza la sensación de victoria alcanzada con la STJUE *Ministerio Fiscal* a la hora de interpretar el ámbito material del art. 1.1 de la Ley 25/2007, sino que coadyuva a nuestra tesis de sostener que el régimen incorporado con la reforma de la LECrim en 2015 merece ser calificado como un «acceso limitado» compatible con la jurisprudencia TJUE, pues frente a la escueta alusión penológica de la Ley 25/2007, la autoridad judicial cuenta ahora con un detallado elenco de criterios legales de ponderación a la hora de determinar la proporcionalidad de la injerencia y decidir qué medidas de investigación puede acordar en función de la gravedad de los hechos objeto de investigación.

Por una parte, el art. 588 bis a) LECrim fija como principios rectores la especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida, especificando el apartado 5º que el canon de proporcionalidad de la medida se resolverá, en cada caso concreto, atendiendo a "la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

Y por otra parte, en la norma procesal española se conjugan dos sistemas legales de delimitación objetiva de la herramienta a utilizar: Uno específico, conforme al cual el uso de específicos instrumentos de investigación se reservan para ciertos listados de delitos (como sucede con el uso del agente encubierto virtual o el registro remoto de equipos informáticos) y uno general, conforme al cual el ámbito objetivo de adopción de las nuevas medidas de investigación queda definido por el juego de los artículos 579.1º y 588 ter a) LECrim[50]. A saber, que se trate de terrorismo o de delitos cometidos en el seno de un grupo u organización criminal; que se trate de delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; o que se trate de delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

En resumen, el régimen recogido en la LECrim, tras su reforma de 2015, debe interpretarse como una derogación tácita de la noción de «delito grave» contenida en el art. 1.1 de la Ley 25/2007[51].

---

[50] TEJADA DE LA FUENTE, E., ZARAGOZA TEJADA, J. I. (2018). Sentencia del tribunal de justicia de la UE (asunto C 207/2016. Ministerio Fiscal): Cuestión prejudicial planteada por la AP de tarragona respecto a los articulos 579.1 y 588 ter a) lecrim y art. 1.º de la ley 25/2007 de 18 de octubre, *Revista Aranzadi Doctrinal*, núm. 11.

[51] Así lo defendíamos en ORTIZ PRADILLO, J. C. (2013). *Problemas procesales…*, op. cit., p. 244.

5. BIBLIOGRAFÍA

CABEZAS, P. (2010). *La investigación del crimen a través de los tiempos*. Tesis doctoral. Universitat Autònoma de Barcelona. Accesible en la dirección URL https://www.educacion.gob.es/teseo/imprimirFicheroTesis.do?idFichero=FIHxYNhGkts%3D. Fecha de consulta: 7 de abril de 2020.

COLOMER HERNÁNDEZ, I. (2018). Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016. En RUDA GONZÁLEZ, A., JEREZ DELGADO, C. (coords.) *Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute*, Madrid: Sepín editorial jurídica.

COLOMER HERNÁNDEZ, I. (2018). La cesión de datos de las comunicaciones electrónicas para su uso en investigaciones criminales: una problemática en ciernes. En JIMÉNEZ CONDE, F. (dir.). Adaptación del derecho procesal español a la normativa europea y a su interpretación por los tribunales. Valencia: Tirant lo Blanch, pp. 77-100.

CRESPO BARQUERO, P. (2010). Intervenciones judiciales en materia de comunicaciones telefónicas e Internet, Cuadernos Penales José María Lidón, núm.7/2010.

DE HOYOS SANCHO, M. (2018). Los efectos expansivos del derecho de la unión Europea sobre las garantías en el proceso penal. En JIMÉNEZ CONDE, F. (dir.). *Adaptación del derecho procesal español a la normativa europea y a su interpretación por los tribunales*. Valencia: Tirant lo Blanch, pp. 43-58.

ENCINAR DEL POZO, M. A. (2014). La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones. SEPIN Top Jurídico, Nuevas Tecnologías, octubre 2014. Referencia: SP/DOCT/18682.

FENECH, M. (1940). El juez y el Nuevo Estado. Barcelona: Bosch.

LÓPEZ BARAJAS, I. (2009). El deber de conservación de datos en la unión europea y sus límites, Revista de Derecho de la Unión Europea, nº 16 - 1er semestre.

MARCHENA GÓMEZ, M. (2011). La vulneración de derechos fundamentales por ministerio de la Ley (a propósito del art. 33 de la Ley General de Telecomunicaciones), *Diario La Ley*, núm. 7572, de 18 de febrero.

MAROTO CALATAYUD, M (2013). Las redes sociales en internet como instrumento de control penal: tendencias y límites. En RALLO LOMBARTE, A., MARTÍNEZ MARTÍNEZ, R. (edit.) *Derecho y Redes Sociales*. Madrid: Civitas, pp. 427-484.

OROMÍ I VALL-LLOVERA, S. (2020). Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE, *Revista de Internet, Derecho y Política*, N.º 31 (Octubre, 2020).

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,* nº 75, Octubre 2010.

ORTIZ PRADILLO, J. C. (2012). Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica. En: PÉREZ GIL (coord.). *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*. Madrid, ed. La Ley, pp. 267-310.

ORTIZ PRADILLO, J. C. (2013). El impacto de la tecnología en la investigación penal y en los derechos fundamentales. En: GONZÁLEZ-CUÉLLAR SERRANO, N. (dir.). *Problemas actuales de la justicia penal.* Madrid: Colex, pp. 317-341.

ORTIZ PRADILLO, J. C. (2013). *Problemas procesales de la ciberdelincuencia*. Madrid: Colex.

ORTIZ PRADILLO, J. C. (2017). Comunicaciones, Tecnología y Proceso Penal: viejos delitos, nuevas necesidades. En ASENCIO MELLADO, J. M. (dir.) *Justicia penal y nuevas formas de delincuencia*. Valencia: Tirant lo Blanch, pp. 15-43.

ORTIZ PRADILLO, J. C. (2017). Desafíos legales de las diligencias de investigación tecnológica. En FUENTES SORIANO, O. (coord.). *EL PROCESO PENAL. Cuestiones fundamentales.* Valencia: Tirant lo Blanch, pp. 303-316.

PÉREZ GIL, J. (2005). Entre los hechos y la prueba: reflexiones acerca de la adquisición probatoria en el proceso penal, *Revista Jurídica de Castilla y León.* n.º 14. enero 2008.

PÉREZ GIL, J. (2010). El nuevo papel de la telefonía móvil en el proceso penal. Ubicación y perfiles de desplazamiento. En: *El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar probar el delito*. Madrid: La Ley.

RODRÍGUEZ LÁINZ, J. L. (2013). Internet de los objetos y secreto de las comunicaciones. *Diario La Ley*, núm. 8034, de 1 de marzo de 2013.

RODRÍGUEZ LÁINZ, J. L. (2014). Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española de conservación de datos relativos a las comunicaciones. *Diario La Ley*, núm. 8308, de 12 de mayo de 2014.

RODRÍGUEZ LÁINZ, J. L. (2017). La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones, *Diario La Ley*, núm. 8901, de 16 de enero de 2017.

SERRANO MASIP, M. (2012). La conservación sistemática y preventiva de datos de tráfico y localización generados por las comunicaciones electrónicas: reacciones contrarias y posible cambio de rumbo en la Unión Europea. En CASTILLEJO MANZANARES, R. (dir.) *Temas actuales en la persecución de los hechos delictivos*. Madrid: La Ley, pp. 437-500.

TEJADA DE LA FUENTE, E. (2017). La conservación de datos informáticos con fines de investigación criminal; requisitos y condiciones para su incorporación al proceso penal. En: ZARAGOZA TEJADA, J. I. (coord.) *Investigación Tecnológica y Derechos Fundamentales. Comentarios a las modificaciones introducidas por la Ley 13/2015*. Cizur Menor: Thomson Reuters Aranzadi, pp. 25-72.

TEJADA DE LA FUENTE, E., ZARAGOZA TEJADA, J. I. (2018). Sentencia del tribunal de justicia de la UE (asunto C 207/2016. Ministerio Fiscal): Cuestión prejudicial planteada por la AP de tarragona respecto a los articulos 579.1 y 588 ter a) lecrim y art. 1.º de la ley 25/2007 de 18 de octubre, *Revista Aranzadi Doctrinal*, núm. 11.

VELASCO NÚÑEZ, E. (2014). Tecnovigilancia, geolocalización y datos: aspectos procesales penales", *Diario La Ley*, núm. 8338, de 23 de junio de 2014.

ZUBOFF, S. (2019). *The Age Of Surveillance Capitalism.* New York: PublicAffairs.