PREMIOS 2023 INSTITUTO VASCO DE DERECHO PROCESAL
AWARDS 2022-2023 BASQUE INSTITUTE OF PROCEDURAL LAW

CONTENIDO / CONTENTS

CESIÓN DE DATOS COMERCIALES RELATIVOS A LAS COMUNICACIONES PARA FINES DE INVESTIGACIÓN CRIMINAL[*]

José Luis Rodríguez Laín[**]
Córdoba

* * *

Es evidente que habría que sacrificar cierto grado
de libertad en beneficio de la justicia y
cierto grado de justicia en beneficio de la libertad".
(BERTRAND RUSSEL. Prólogo a la Tercera Edición,
versión en inglés, de *"Los caminos de la Libertad"*, junio de 1948)

I- EL ORIGEN: LOS DATOS RELATIVOS A LAS COMUNICACIONES ELECTRÓ-

---

[*] El trabajo ha obtenido el Premio Instituto Vasco de Derecho Procesal en su XIII Edición del año 2023.
[**] José Luis Rodríguez Laín es Magistrado titular del juzgado de Instrucción 4 de Córdoba.

TRÓNICAS COMO FUENTE DE INVESTIGACIÓN CRIMINAL[1]

Todo comenzó cuando en agosto de 1984 el Tribunal Europeo de Derechos Humanos –TEDH- hubo de enfrentarse por primera vez a una realidad tecnológica que permitía sacar cierto partido a la investigación criminal a través del análisis de datos de tráfico de comunicaciones ya consumadas, y no necesariamente objeto de previo seguimiento en tiempo real. Del rudimento del *comptage* o *metering*, bien en base a la capacidad innata de ciertos funcionarios policiales para calcular mentalmente el tiempo que tardaba el dial de un teléfono intervenido en retornar al punto de reposo, bien al empleo de herramientas mecánicas que sustituían a aquéllos de una forma más fiable[2], se había pasado a la comodidad de poder solicitar al correspondiente prestador del servicio de telefonía una información detallada sobre cuestiones tan relevantes como números de abonado con el que un determinado terminal telefónico hubiera contactado, tanto como emitente como receptor, en un determinado período de tiempo, datación y duración de la llamada.

La STEDH de 4 de agosto de 1984 (caso MALONE v. Reino Unido, asunto 8691/79) asumió este reto, enfrentándose a un supuesto de hecho en el que el Sr. Malone imputaba a las autoridades policiales británicas haber accedido durante años a información detallada sobre sus contactos telefónicos; siendo una de las posibilidades técnicas para que ello hubiera podido tener lugar, al haberse negado por las autoridades británicas la existencia de más interceptaciones que las correspondientes a un breve período de tiempo, precisamente la de acudir al prestador de telecomunicaciones para que facilitara dicha información almacenada por éste por razones comerciales.

Sin perjuicio de realizar la comprometida afirmación de que el examen, tras su cesión, de la información referida a lo que en el futuro fueran definidos como datos de tráfico, aunque de diferente naturaleza, comportaba una afectación del derecho al respeto de la correspondencia, garantido como tal por el art. 8.1 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales, de 4 de noviembre de 1950 –CEDH-[3], el Alto Tribunal Europeo concluirá realizando una importante aportación sobre la conformidad con dicho precepto de las prácticas de las operadoras de telecomunicaciones de conservar y tratar tales datos, en tanto en cuanto ello fuera preciso para la prestación del ser-

[1] El presente trabajo forma parte del Proyecto PID2022-137826NB-I00 financiado por el Ministerio de Ciencia e Innovación-Agencia Estatal de Investigación sobre *"Datos personales e información en la era digital: desafíos en su obtención y uso en los procesos judiciales y en los procedimientos sancionadores (DATER)"*.

[2] El *meter check printer* era un dispositivo empleado por las autoridades policiales británicas para descubrir los contactos telefónicos de un determinado terminal objeto de interceptación legal. El dispositivo no solo permitía identificar de forma mecánica los números de teléfono marcados por el dispositivo, sino también fecha y duración de las llamadas. Véase sobre el particular el § 56 de la STEDH de 4 de agosto de 1984 (caso MALONE v. Reino Unido; asunto 8691/79).

[3] *"The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8".*

vicio –§ 84-[4]. Era legítimo, por tanto, que las operadoras trataran estos datos a los efectos de dar respuesta a las finalidades legítimas de su captación y conservación; no pudiendo negarse, en consecuencia, como sucediera en el precedente de la sentencia del caso MALONE v. Reino Unido, que las autoridades competentes pudieran recabar tal información de aquéllas en el contexto de una investigación criminal, en tanto que la decisión pudiera tener cabida dentro del margen de actuación que determinara el apartado 2 de dicho precepto del CEDH.

Ya dentro del universo de las comunicaciones electrónicas, el mismo planteamiento sería reproducido, entre otras, diecisiete años después, por la STEDH, Secc. 3ª, de 25 de septiembre de 2001 (caso P.G. y J.H. v. Reino Unido; asunto 44787/98)[5]. La idea de que las operadoras de comunicaciones electrónicas estarían legitimadas para el almacenamiento y tratamiento de estos datos, siempre siguiendo un referente de finalidad o funcionalidad, y que la información así tratada pudiera tener acceso a una investigación criminal, encontraba un firme sustento en la jurisprudencia del TEDH. Solamente en supuestos en los que la fuente de conocimiento tuviera un origen diverso a la prestación de un servicio de telecomunicaciones, y pudiera esgrimirse por el usuario afectado por la injerencia una situación de expectativa razonable de privacidad, especialmente en el ámbito de las relaciones laborales, este posible almacenamiento y uso sí podría confrontarnos con una transgresión del art. 8.1 del CEDH; tal y como nos indicaran las célebres SSTEDH, Secc. 4º, de 3 de abril de 2007 (caso COPLAND v. Reino Unido; asunto 62617/00), y, Gran Sala, de 5 de septiembre de 2017 (caso BĂRBULESCU v. Rumanía, 61496/08).

El análisis de los datos que son tratados y conservados por las operadoras de comunicaciones electrónicas o prestadores de servicios de la sociedad de la información, que tienen por objeto canalizar el intercambio de información entre personas, ha adquirido de manera cada vez más creciente un importantísimo papel en la investigación criminal. La interceptación de comunicaciones en tiempo real presupone la identificación del sospechoso y el encauzamiento de una investigación concreta contra éste y por supuesta infracción criminal, con propensión de expandir su propia dinámica o efectos en el futuro, solamente atañe a un número muy limitado de supuestos. La investigación criminal es, casi por definición, un proceso de indagación que afecta a hechos del pasado; y ello no hace sino reproducirse de forma muy marcada en la investigación de hechos ya acontecidos, bien en un escenario tecnológico, bien en un escenario real, pero que permiten ser esclarecidos gracias a un adentramiento en una realidad tecnológica como fuente de obtención de evidencias. Podemos identificar al autor de una estafa por Internet si descubrimos la IP que le fuera asignada al colgar en un popular portal de anuncios una oferta falsa de alquiler de un apartamento vacacional en Benidorm; o facilitar la identidad del autor de un brutal atentado terrorista en un tren de cercanías gracias al recabo de información sobre los IMSI de terminales telefónicos móviles bajo la cobertura de una estación de telefonía móvil tipo BTS en determinada franja de tiempo. En ambos supuestos la colaboración del prestador que almacenara legítimamente dichos datos sería tanto o más importante que una posible interceptación de comunicaciones que partiría de su imposible anticipación.

II. EL ESCENARIO DEL DERECHO DE LA UNIÓN EUROPEA

[4] *"As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service".*

[5] En igual sentido se pronunciará la STC 123/2002, de 20 de mayo.

La Directiva 95/46/CE[6] representaría la definitiva apuesta del legislador comunitario por someter a regulación el complejo y cambiante ámbito regulatorio de la protección de datos de carácter personal. Si el TEDH analizó la legitimidad del almacenamiento y tratamiento de datos relacionados con telecomunicaciones en un contexto de funcionalidad, la Directiva 95/46/CE, frente al precedente del Convenio Europeo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal de 1981, avanzará no solo reconociendo la trascendencia del principio del consentimiento al tratamiento, sino su clara preponderancia. Así se podía apreciar de la lectura de su art. 7; colocando en primer lugar al consentimiento del interesado entre los criterios que legitiman al tratamiento de datos. Por supuesto que ese criterio de funcionalidad anticipado por la jurisprudencia del TEDH encontraría igualmente un reconocimiento en el apartado b) del mismo precepto; pero esa evidente preponderancia del principio del consentimiento marcaría claramente toda la estructura de la norma comunitaria. El tratamiento de datos relativos a las comunicaciones no era considerado en modo alguno como una excepción. Además, el art. 13 desarrollaba un régimen jurídico que permitía excepcionar el ejercicio de determinados derechos de los ciudadanos relacionados con la protección de sus datos personales en razón de un interés público superior; entre los que se encontraba *"la prevención, la detección y la represión de infracciones penales"* -art. 13.1,d)-.

Pronto el legislador comunitario fue consciente de la urgencia de abordar el tratamiento de datos relacionados con comunicaciones electrónicas como una especialidad frente a dicha normativa[7]. Tráfico internacional de datos, constante evolución de las tecnologías de las comunicaciones y potencialidad de afectación de derechos fundamentales de los usuarios consecuencia de la necesaria intermediación de prestadores de servicios de comunicaciones electrónicas, estaban detrás de esta necesaria revolución normativa. Es en este contexto donde surgirá una norma, la Directiva 2002/58/CE[8], con vocación de regular la protección de datos en el ámbito de las comunicaciones electrónicas; haciéndolo, además, con el claro cometido de convertir el criterio de funcionalidad en el almacenamiento y tratamiento de datos en prevalente, frente a un consentimiento que pasaba a ser auténticamente gregario de aquél.

Uno de los cometidos esenciales de la Directiva, nos dirá su art. 5.1, sería el de garantizar *"…la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público"*; aunque para ello el mismo precepto se mostrara comprensivo de la necesidad del tratamiento técnico de los datos de tráfico por parte de los prestadores de servicios, sometidos a un mismo principio de confidencialidad común a los contenidos de comunicaciones[9]. Y es de aquí de donde parte la norma para desarrollar en sus

[6] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

[7] El art. 1.2 de la Directiva 2002/58/CE, a la que seguidamente haremos mención, sentará con claridad esta naturaleza especial de la norma en relación con el tronco común de la Directiva 95/46/CE. Establecía, de hecho, que: *"Las disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE a los efectos mencionados en el apartado 1…".*

[8] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

[9] *"El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad".*

arts. 6 y 9 ese marcado principio de funcionalidad que llega a lastrar severamente cualquier posibilidad de obtener del usuario un consentimiento lícito a un tratamiento más allá de las necesidades propias de la prestación del servicio demandado.

El tratamiento de los datos de tráfico –art. 6-, comienza con un incontestable sometimiento a ese principio de funcionalidad; de suerte que la regla general será la de que solamente se permita el tratamiento de datos de tráfico generados por las comunicaciones mantenidas por abonados y usuarios en tanto ello fuera preciso para la transmisión de una comunicación. A partir de la pérdida de esa funcionalidad, nos dirá el apartado 1 de dicho precepto, el destino de los datos no podría ser otro que el de su destrucción o anonimización. Ahora bien, la propia norma intenta relajar tan estricta limitación; definiendo otras situaciones en las que, bien por las necesidades propias de la relación contractual, bien por abrirse a la posibilidad de cierta condescendencia con la irrupción del principio del consentimiento, se desvanecerá el nudo criterio de la estricta funcionalidad a los efectos de canalización de una concreta comunicación. Por una parte, determinados datos de tráfico habrían de poder ser conservados en tanto en cuanto ello fuere preciso a los efectos de *"…la facturación de los abonados y los pagos de las interconexiones"*; lo que permitiría su almacenamiento y tratamiento al menos hasta el momento en que expirara el plazo durante el cual pudiera legalmente impugnarse la factura o exigirse el pago[10]. Promoción comercial y prestación de servicios de valor añadido[11]

[10] Determinar realmente cuáles son estos plazos tanto de reclamaciones por parte de los abonados como de posible ejercicio de acciones de cobro de facturas impagadas nos enfrenta a un complejo dilema jurídico. El art. 27 del Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas, es la norma que en un principio disciplinaría el cauce de reclamación de los abonados frente a decisiones de operadoras de telecomunicaciones; entre las que sin duda estaría la reclamación frente a facturas emitidas. La norma presupone un previo procedimiento de reclamación directa ante los servicios de atención al cliente de la propia operadora; en un contexto en el que cada Comunidad Autónoma, en el ejercicio de sus competencias propias en materia de consumo, podría establecer procedimientos específicos de resolución de controversias. Realmente, solo se regula un trámite administrativo de reclamación ante la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información; en el que intervendría como órgano con capacidad de resolución la División de Atención al Usuario de Telecomunicaciones -art- 8.3 del Real Decreto 1554/2004, de 25 de junio, por el que se desarrolla la estructura orgánica básica del Ministerio de Industria, Turismo y Comercio-. El apartado 2 de dicho art. 27, sin perjuicio de prever la aprobación de una Orden Ministerial que regulará el procedimiento, aún no aprobada, establece un plazo único de seis meses para resolver y notificar la resolución. Sí existe una Orden Ministerial preexistente al referido RD 899/2009; y que, a falta de desarrollo de dicho mandato reglamentario, deberíamos considerarla en vigor: la Orden ITC/1030/2007. Al menos en aquellas Comunidades Autónomas en que no se hubiera desarrollado una normativa propia debería ser considerada ésta como norma aplicable. En ella se establece un procedimiento previo de reclamación para finalidades concretas desarrolladas en su art. 3 (prácticamente todos los ámbitos imaginables, a excepción de reclamación de indemnizaciones por fallos del servicio o impugnación de cláusulas que pudieran considerarse por el abonado abusivas); y se marca como plazo para la reclamación el de un mes *"…desde el momento en que se tenga conocimiento del hecho que motiva la reclamación"*; que abriría un plazo de otro mes para recibir la respuesta de la operadora o para abrir el camino a la reclamación en sede administrativa. Ello, como podemos fácilmente apreciar, supone un solapamiento de plazos que dificulta seriamente la determinación concreta de unos plazos de legítima conservación, difícilmente conciliables con una legislación administrativa en materia de sentido del silencio por no respeto de los plazos de resolución que no está pensada para solventar conflictos jurídicos entre particulares; y que, además, no debería cerrar definitivamente las puertas para que un ciudadano, insatisfecho ante la respuesta de su operadora de telecomunicaciones ante una reclamación sobre facturación, pudiera acudir a la jurisdicción civil, con evidentes lagunas jurídicas sobre cuál sería en tal supuesto el momento del inicio del cómputo del

representarán, conforme al apartado 3 del mismo precepto un claro ejemplo de reconocimiento de un tímido resurgimiento del principio del consentimiento. Pero de nuevo se ven sometidos a un recurrente criterio de funcionalidad: *"…en la medida y durante el tiempo necesarios para tales servicios o promoción comercial"*.

Cuando hablamos de datos de localización distintos a los datos de tráfico[12], la estrategia del legislador comunitario se centra en un criterio de exclusiva aplicación del principio del consentimiento como base de la captación misma del dato para la prestación del concreto servicio que se ofrece al usuario. Ya no estamos hablando de un consentimiento que se presupone, ni de un legítimo derecho del prestador a tratar unos datos que son precisos para dar el servicio concertado con el abonado. Los servicios de valor añadido que requieren de estos datos de localización distintos a los de tráfico han de ser expresamente demandados y/o acepta-

plazo de prescripción de la acción de reclamación. Para complicar aún más el laberinto normativo, el RD 899/2009 derogaba el art. 104.2 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios; norma que sí establecía plazos concretos para la presentación de la reclamación ante la operadora (un mes, según su apartado 1) y ante la Administración (tres meses, según el apartado 4, si es que no se hubiera acudido a una Junta Arbitral de Consumo conforme a su normativa específica). La posición de la operadora ante impagados ampliaría aún más el tiempo de conservación hasta los límites de la prescripción de la acción de reclamación; toda vez que una posible legítima oposición del abonado, basada en el cuestionamiento de conceptos de la facturación y/o en la ausencia de comunicación de las facturas conforme al régimen pactado por las partes, convertiría la conservación de los datos precisos para el cálculo de la misma en legítima.

[11] El art. 2,g) de la Directiva define al servicio de valor añadido como: *"Todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación"*. El considerando décimo octavo recoge como ejemplos de servicios de valor añadido las recomendaciones sobre tarifas menos costosas, orientación vial, información sobre tráfico, previsiones meteorológicas e información turística. Siguiendo el ejemplo de la información sobre tráfico, la ubicación vía GPS o a través de posicionamientos en contacto con redes Wi-FI es compartida con el prestador del servicio; quien ubica al dispositivo móvil en la cartografía empleada, sugiriendo rutas o facilitando la llegada al destino solicitado por el usuario. El dato de geoposicionamiento no es extraído por el prestador del servicio como consecuencia de un tráfico de comunicaciones, sino por la compartición por el usuario del dato que genera su dispositivo en función a su localización geográfica.

[12] La Directiva 2002/58/CE no incluye un concepto específico de datos de localización distinto de los de tráfico. Para comprender su significado, que ya hemos anticipado en buena parte en la nota a pie de página anterior, hemos de acudir El art. 2,c) de la Directiva; donde se define a los datos de localización como: *"cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público".* En base a un simple criterio de exclusión, habríamos de concebir el dato de localización distinto al de tráfico como aquél que no se genera como consecuencia de la prestación de un servicio de comunicaciones a los usuarios. La geolocalización generada de forma automática o por activación de una aplicación (vgr., compartición de geoposicionamiento a través de programa específico como el popular *Latitude*, utilidades de Google Maps o por transmisión de la ubicación a través de la aplicación WhatsApp) por el propio dispositivo de comunicaciones sería el ejemplo paradigmático de dato de localización distinto del de tráfico. Por el contrario, no entrarían en esta definición, aunque no participen directamente en un proceso comunicativo, los datos de localización precisos para garantizar la conectividad del dispositivo con la red de comunicaciones; como sucederá con la referencia a conexión con estación BTS, y el posible encuadramiento de dirección y distancia en función del grado del ángulo en que se posicione el dispositivo de entre los tres en que se subdivide la estación y el segmento de distancia respecto de ésta.

dos por el abonado o usuario; y solo en base a ese consentimiento, precedido de una adecuada información sobre el tratamiento y su alcance, surgirá la posibilidad de acceso y tratamiento a los mismos, de nuevo en un contexto de previa anonimización, o en la medida y por el tiempo necesarios para la prestación del servicio -art. 9.1-.

El art. 15.1 de la Directiva 2002/58/CE se convertirá en la clave esencial para la priorización de determinados intereses públicos, entre los que obviamente se encontraría la investigación de infracciones criminales, frente al férreo principio de confidencialidad afectante a contenidos y datos de tráfico de comunicaciones electrónicas, así como datos de localización. El diseño del precepto difiere en parte del esquema propuesto por el art. 13 de la Directiva 95/46/CE: Ya no se piensa tanto en permitir la excepción de determinados derechos de los ciudadanos en el torno de la protección de sus datos personales, sino en establecer, como consecuencia de una excepción o suspensión temporal a este principio, una habilitación a los Estados miembros de la Unión para poder regular determinadas medidas de injerencia afectantes en términos generales al concepto amplio de privacidad, tanto a nivel de su definición normativa como de aplicación de éstas en el caso concreto.

El Reglamento (UE) 2016/679[13] -RGPD- surge ante la necesidad de adaptar la vetusta Directiva 95/66/CE a la incesantemente cambiante realidad del tratamiento de datos personales. La decidida expansión de los principios relacionados con la legitimidad del tratamiento y el consentimiento es evidente. Pero no deberíamos obviar la realidad de que el propio RGPD, en su art 95, vuelve a recalcar ese carácter de norma especial que mantiene la Directiva 2002/58/CE en cuanto respecta al tratamiento de datos relacionados con las comunicaciones electrónicas. Que el RGPD haya, inevitablemente, de penetrar en dicha regulación especial es algo jurídicamente inevitable; pero el precepto limita tal penetración, en tanto que concretas disposiciones del Reglamento supusieran la imposición de *"...obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE"*.

El mismo sentido habría de darse a la Directiva (UE) 2016/680[14]; la cual presupone en sí misma la existencia de la excepción al principio del consentimiento, tratando a toda costa de garantizar estándares de protección de los derechos de los ciudadanos frente a inmisiones legítimas, por parte de los poderes públicos, en sus derechos relacionados con la protección de datos personales.

III) LAS EXCEPCIONES AL PRINCIPIO DEL CONSENTIMIENTO: CONSERVACIÓN PREVENTIVA, RETENCIÓN POR DECISIÓN DE AUTORIDAD COMPETENTE Y CESIÓN DE DATOS CONSERVADOS POR MOTIVOS COMERCIALES

[13] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

[14] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

La Directiva 2002/58/CE nace en un escenario realmente convulso; forzada por las presiones de determinados Estados miembros de la Unión Europea que veían en la conservación preventiva de datos relativos a las comunicaciones una herramienta, no solo útil, sino indispensable en la lucha contra determinadas modalidades de delincuencia, especialmente el terrorismo y el crimen organizado. La referencia que se hace en el último inciso de su art. 15.1 a la posibilidad de que los Estados miembros pudieran adoptar, *"…entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado…"* justificadas por alguna de las finalidades legítimas que prevé la norma, no podía ser más clara en este sentido[15]. Era una intención del legislador europeo precisamente facilitar que a nivel interno pudiera regularse esta excepción; lo que, como consecuencia de los atentados terroristas de Londres de 7 de julio de 2005, se traduciría en la aprobación de una controvertida norma, la Directiva 2006/24/CE[16], que imponía a los Estados miembros de la Unión la regulación uniforme de sistemas de conservación preventiva de datos conforme a las normas de mínimos que se fijaban. La nueva Directiva se plantearía sortear las dificultades y trabas que imponía la regulación de la materia desde la perspectiva del entonces llamado Tercer Pilar; y que estuviera detrás del fracaso de un primer intento de regulación uniformadora sobre la materia, vía Decisión Marco[17]. Pero lo haría, desplegando toda su astucia, desplazando la base normativa de la norma hacia el ámbito no sometido a unanimidades ni mayorías cualificadas de la armonización de normas en materia de prestación de servicios en el ámbito del Derecho de la Unión.

En esta decisión del legislador europeo se escondía el germen de su ulterior estrepitoso fracaso; frente a una jurisprudencia del Tribunal de Justicia de la Unión Europea -TJUE-, que finalmente trató la norma como si precisamente una regulación del ámbito del Espacio de Libertad, Seguridad y Justicia se tratara. Si bien en la STJUE (Gran Sala) de 10 de febrero de 2009 (caso IRLANDA v. Parlamento y Consejo; asunto C-301/06), se consigue salvar el óbice formal de la elección del instrumento normativo, la STJUE (Gran Sala) de 8 de abril de 2014 (caso DIGITAL RIGHTS IRELAND y SEITLINGER y otros; asuntos C-293/12 y C-594/12), supuso, como de todos es sabido, la declaración de invalidez íntegra de todo el texto normativo; inaugurando toda una panoplia de ulteriores resoluciones que una y otra vez volvían al mismo argumento de afirmar de forma contundente la contrariedad con el Derecho de la Unión de regímenes legales de conservación preventiva de datos relativos a las comunicaciones, salvo muy contadas excepciones. A la eliminación del acervo comunitario de esta Di-

[15] Sobre los antecedentes e hitos previos a la publicación de la Directiva 2006/24/CE, así como su ulterior evolución jurisprudencial, puede consultarse el trabajo de RODRÍGUEZ LAINZ, José Luis: *"La definitiva defenestración de la ley española sobre conservación de datos relativos a las comunicaciones"* (Diario La Ley Nº 8901, Sección Doctrina, 16 de enero de 2017).

[16] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

[17] Proyecto de resolución legislativa del Parlamento Europeo sobre la iniciativa de la República Francesa, de Irlanda, del Reino de Suecia y del Reino Unido relativa a un proyecto de Decisión Marco sobre la conservación de los datos tratados y almacenados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de los datos transmitidos por redes públicas de comunicaciones, a efectos de la prevención, investigación, descubrimiento y represión de la delincuencia y las infracciones penales, con inclusión del terrorismo (8958/2004 – C6-0198/2004 – 2004/0813(CNS)).

rectiva, pese a la posición favorable de una representativa parte de la doctrina[18] y jurisprudencia nacional[19], como de un amplio elenco de Estados miembros, se añadiría una segunda resolución, la STJUE (Gran Sala) de 21 de diciembre de 2016 (caso TELE2 SVERIGE AB y otros; asuntos C-203/15 y C-698/15) la cual dejaría bien claro que el interés del Derecho de la Unión en la salvaguardia de la privacidad de las personas abarcaba también a regulaciones nacionales que impusieran con carácter generalizado y preventivo tal deber de conservación para finalidades propias de la lucha contra la delincuencia; y ello por afectación no solo del art. 15.1 de la Directiva 2002/58/CE, sino por comprometer a derechos fundamentales tales como los garantidos en los arts. 7, 8, 11 y 52.1 de la Carta de Derechos fundamentales de la Unión Europea -CDFUE-.

Si ya la segunda de las sentencias citadas abría las puertas a determinados regímenes de retención selectiva de datos en un contexto de lucha contra la delincuencia, de prevención y persecución del delito y los delincuentes, será la sentencia de los casos TELE2 SVERIGE AB y otros, la que marcará el origen de esta distinción que está generando cierto grado de confusión tanto a nivel doctrinal como de aplicación por nuestra jurisprudencia nacional. Dedicaremos los cuatro siguientes subapartados a aclarar y desarrollar estos dos conceptos, como claramente diversos a la técnica de cesión de datos conservados por las operadoras de comunicaciones por motivos comerciales; confrontándolos con las órdenes de preservación rápida -*quick freezing orders*- y las nuevas formas de conservación/denuncia por iniciativa de proveedores de servicios de Internet, de origen legal.

A) El régimen de conservación preventiva de datos: De la defenestración a su tímido renacer; pasando por la lenta agonía de la situación del ordenamiento jurídico español

El régimen de conservación preventiva de datos a las resultas de una eventual utilización procesal no supone otra cosa que un deber que se impone a determinadas operadoras de conservar de forma indiscriminada y generalizada categorías datos relativos a las comunicaciones por ellas gestionados con motivo de la prestación de servicios de comunicaciones electrónicas, o, desde la publicación de la Directiva (UE) 2018/1972[20], a distintas formas de

[18] Pueden citarse en este sentido trabajos como los publicados por MARCHENA GÓMEZ, Manuel y GONZÁLEZ-CUÉLLAR SERRANO, Nicolás: *"La reforma de la Ley de Enjuiciamiento Criminal en 2015"*; Ediciones Jurídicas Castillo de Luna; primera edición, Madrid noviembre 2015, págs. 295 y 296; aunque proponiendo una adecuada reforma de la ley española de conservación de datos. En contra: ENCINAR DEL POZO, Miguel Ángel: "*La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones"* (Top Jurídico, Nuevas Tecnologías, octubre 2014. Editorial SEPIN; Referencia: SP/DOCT/18682); así como CABEZUDO RODRÍGUEZ, Nicolás: *"Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal"*; en I Jornada del Boletín del Ministerio de Justicia: Las Reformas del Proceso Penal; Boletín del Ministerio de Justicia, Año LXX, Núm. 2186, febrero 2016, pág. 51.

[19] Tal posición jurisprudencial encontró como punto de arranque a la STS 470/2015, de 23 de noviembre.

[20] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo de 11 de diciembre de 2018 por la que se establece el Código Europeo de las Comunicaciones Electrónicas. El Considerando 7 de la Directiva pone como ejemplos de ello *correo web* y *los servicios de mensajería*. La STJUE (Gran Sala) de 6 de octubre de 2020 (caso LA QUADRATURE DU NET y otros; asuntos C-511, 512 y 520/18), con cita del precedente de la STJUE, Sala Cuarta, de 5 de junio de 2019 (caso SKYPE COMMUNICATIONS; asunto C-142/18), llega a considerar en su parágrafo 204 que los servicios de la sociedad de la información consistentes en el alojamiento y tratamiento de datos están sometidos al mandato de la Directiva

canalización de comunicaciones por prestadores de determinados servicios de Internet: los *servicios de comunicaciones interpersonales independientes de la numeración* a que se refiere la mencionada Directiva a las que se someterá de forma indirecta, casi por la puerta de atrás, a la férrea disciplina de la Directiva 2002/58/CE[21].

Se trata por ello de una conservación generalizada e indiscriminada que no conoce más límites que los márgenes temporales que se imponen por la norma que regula tal deber de conservación. Pero si una característica es genuina de esta forma de conservación de datos es precisamente la de que su origen es exclusivamente legal. Es una norma con rango de ley o equiparable, y no una decisión de una concreta autoridad judicial o administrativa, el fundamento mismo de ese deber de conservación. La intervención de una u otra se hace depender de una concreta orden de cesión de determinados datos que resulten precisos en el contexto de una investigación criminal o a los efectos de darles destino para alguna de las finalidades legítimas que establece la norma reguladora.

Las leyes que, dentro del ámbito de influencia de la Directiva 2006/24/CE, regulaban tales bases de datos partían del denominador común de mostrarse estrictas en orden a definir plazos de conservación genéricos o según la naturaleza del dato; limitar la accesibilidad de los datos solo a la investigación de determinadas infracciones criminales, generalmente categorizadas por un cierto nivel de gravedad del delito en función de su penología; determinar las autoridades con capacidad para beneficiarse de la cesión de datos, así como establecer férreas medidas de seguridad como garantía de impedir el acceso de personas no autorizadas a tales inmensas fuentes de información y minimizar riesgos de su manipulación o destrucción, incluidas la designación de órganos independientes de control.

Como es sabido, la STJUE (Gran Sala) de 8 de abril de 2014 (casos DIGITAL RIGHTS IRELAND y SEITLINGER y otros; asuntos C-293/12 y C-594/12) declaró la incompatibilidad con el Derecho de la Unión de la Directiva 2006/24/CE en la que se ampararan los Estados miembros para regular estas bases de datos a nivel interno. Bajo la apreciación de una grave afectación del principio de proporcionalidad en la restricción de derechos fundamentales del orden de la confidencialidad de las comunicaciones y la protección de datos de carácter personal, la sentencia llegó a establecer lo que aparentaban ser unos criterios o contenidos mínimos de la norma que permitieran soslayar esa preocupación que se presumía en la ciudadanía de verse compelidas a restringirse en el uso de herramientas de comunicación electrónica como consecuencia de posibles excesos en la utilización por los poderes públicos o terceros de tan ingente información; y ello por el solo hecho de ser ciudadanos que interactuaban a través de las redes de comunicaciones. Tales exigencias, que orbitaban sobre la imperiosa necesidad de respeto del afectado principio de proporcionalidad, se desgranaron en una mejor perfilación del concepto de delito grave que abría las puertas a su posible cesión y uso de los datos almacenados; la definición de normas procesales, en un procedimiento bajo la autorización o control de una autoridad judicial o administrativa independiente; la definición de plazos de conservación, que habrían de ajustarse a la naturaleza de los datos sometidos a deber de conservación, y el establecimiento de las correspondientes medidas de salvaguardia de

2002/58/CE. Ello incluiría, sin duda, a los *servicios de mensajería en Internet*, nos dirá el parágrafo siguiente.

[21] En este sentido: RODRÍGUEZ LAINZ, José Luis: *"Reflexiones sobre el tratamiento de datos personales por prestadores de servicios de comunicaciones vía internet para la lucha contra abusos sexuales de menores en línea en el Reglamento (UE) 2021/1232".* Diario La Ley, Nº 9974, 20 de diciembre de 2021, Wolters Kluwer.

la información almacenada, bajo el control y supervisión externos de una autoridad independiente.

Los Estados miembros de La Unión vieron en la norma excepcional del art. 15.1 de la Directiva 2002/58/CE, una oportunidad para mantener la vigencia de estas leyes nacidas al abrigo de la fracasada Directiva 2006/24/CE; aprovechándose para ello, por una parte, de la interpretación posible de la STJUE de 8 de abril de 2014 en el sentido de que una norma nacional respetuosa con las exigencias desarrolladas por la misma podría superar el óbice de afectación del principio de proporcionalidad denunciado, y en la razonable consideración de que la pérdida de vigencia de una norma comunitaria no supondría necesariamente la pérdida de vigencia de las normas nacionales dictadas en su implementación, en tanto en cuanto no fueran éstas contrarias a otra norma del acervo comunitario. La jurisprudencia de la Sala 2ª del Tribunal Supremo abrazó rápidamente tal planteamiento en sentencias tales como las SSTS 470/2015, de 7 de julio; 768/2015, de 23 de noviembre; 272/2017, de 18 de abril; 400/2017, de 1 de junio, y 723/2018, de 23 de enero de 2019 defendiendo todas, la plena vigencia de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones -LCDCE-.

Sin embargo, la publicación de la STJUE (Gran Sala) de 21 de diciembre de 2016 (casos TELE2 SVERIGE AB y otros; asuntos C-203/15 y C-698/15) daría comienzo a lo que aparentaba ser un camino sin retorno hacia la definitiva defenestración de regímenes legales de conservación de datos. La sentencia, de hecho, haciendo frente a una legislación sueca que mostraba un destacado mimetismo con el ejemplo de la ley española, la LCDCE, llegaba a una contundente conclusión que aparentaba no ofrecer ningún resquicio en el que poder apoyar la conformidad con el Derecho de la Unión: dicho art. 15.1 de la Directiva 2002/58/CE, en relación con los arts. 7, 8, 11 y 52.1 de la CDFUE se oponía a una norma nacional *"…que establece, con la finalidad de luchar contra la delincuencia, 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"*.

La jurisprudencia del TJUE se mantuvo firme en todo momento en tal posicionamiento. Así lo haría frente a cuestiones prejudiciales en las que los órganos judiciales proponentes la enfrentaron a los ejemplos de la lucha contra determinadas fenomenologías de delincuencia especialmente grave, como ocurriera en el supuesto de la legislación francesa con el ejemplo del terrorismo o la salvaguardia de intereses financieros de alcance comunitario -SSTJUE (Gran Sala) de 6 de octubre de 2020 (caso LA QUADRATURE DU NET y otros; asuntos C-511, 512 y 520/18), y (Gran Sala) de 20 de septiembre de 2022 (caso COUR DE CASSATION, asuntos C-339/20 y C-397/20)-; o contra delitos de especial gravedad, como fuera un asesinato, en el caso de la legislación irlandesa -STJUE (Gran Sala), de 5 de abril de 2022 (caso G.D. y COMISSIONER AN GARDA SÍOCHÁNA; asunto C-140/20)-. Pero tampoco cuando se la confrontara con la limitación más o menos laxa de los plazos de conservación, como la legislación de Estonia -STJUE (Gran Sala) de 2 de marzo de 2021 (caso PROKURATUR; asunto C-746/18)-, o incluso especialmente restrictiva, como la alemana -STJUE (Gran Sala) de 20 de septiembre de 2022 (casos SPACENET AG y TELEKOM DEUTSCHLAND GMBH: asuntos C-793 y 794/19).

Sin embargo, la jurisprudencia del Tribunal Supremo, en sentencias tales como las SSTS 727/2020, de 23 de marzo de 2021, y 824/2022, de 19 de octubre, se mostraba firme en unos planteamientos iniciales; en los que, insistiendo de nuevo en la capacidad de adaptación de la ley española y su aplicación jurisprudencial, se añadían nuevos argumentos basados en lo que se consideraba posibilidad de respeto del principio de primacía y equivalencia del De-

recho de la Unión; el afianzamiento de la opción del legislador nacional por la vigencia de la LCDCE en normas posteriores, como el art. 42 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones –LGT-[22]; la apuesta por la aplicación del principio adversarial como forma de mantener la validez de evidencias obtenidas mediane el acceso a las bases de datos de la LCDCE, y el reconocimiento de un carácter evolutivo de la jurisprudencial del TJUE que no le llevaba, sin embargo, a plantearse la necesidad de acudir a la vía de la cuestión prejudicial.

La publicación en el mismo día de las SSTJUE (Gran Sala) de 6 de octubre de 2020 (caso LA QUADRATURE DU NET y otros; asuntos C-511, 512 y 520/18), y (Gran Sala) de 6 de octubre de 2020 (caso INVESTIGATORY POWERS TRIBUNAL; asunto C-623/17) supuso el punto de inflexión en un cambio de rumbo en la cerrazón anterior del TJUE al reconocimiento de cualquier forma y supuesto de regímenes de conservación preventiva. El cambio se producirá, sin embargo, desde la exploración de nuevas vías y la consideración de determinados datos como esenciales para el inicio de cualquier investigación de naturaleza tecnológica y/o la menor gravedad de la injerencia que podría presuponerse de su conservación y ulterior cesión.

Si la autoridad judicial francesa expondría al TJUE a la necesidad de dar una respuesta a la lucha contra el terrorismo, la autoridad británica saca a relucir unos sistemas de *inteligencia extranjera* que, a través de las denominadas técnicas de *bulk interception,* permitían en Estados pertenecientes a la Unión Europea, monitorizar, almacenar y tratar el tráfico de comunicaciones provenientes del extranjero para determinadas finalidades relacionadas con la seguridad y la defensa nacional; sin duda bajo la influencia ya de las SSTEDH, Secc. 3ª, de 19 de junio de 2018 (caso CENTRUM FÖR RÄTTVISA v. Suecia; asunto 35252/08), y Secc. 5ª, de 13 de febrero de 2018 (caso BIG BROTHER WATCH y otros v. Reino Unido; asuntos 58170/13, 62322/14 y 24960/15)[23]. Aunque con severas salvaguardias en su regulación y aplicación, el TJUE se verá en la obligación de claudicar y mostrarse favorable a conciliar con el art. 15.1 de la Directiva 2002/58/CE regímenes por los cuales, y a efectos de la protección de la seguridad nacional, se permitiera la emisión de requerimientos a los proveedores de servicios de comunicaciones electrónicas para que procedieran a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en situaciones en las que el Estado miembro en cuestión se enfrentara a una amenaza grave para la seguridad nacional que resultara real y actual o previsible. Las salvaguardias consistirían en la imposición de un control efectivo por parte de autoridad judicial o administrativa independiente*, "…cuya decisión tenga carácter vinculante, que tenga por objeto comprobar la existencia de una de estas situaciones, así como el respecto de las condiciones y de las garantías que deben establecerse, y teniendo en cuenta que dicho requerimiento únicamente podrá expedirse por un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse en caso de que persista dicha amenaza"*. Como podemos ver, nos enfrentamos a regímenes de conservación preventiva de datos; pero su fuente no es directamente una norma legal, sino una decisión tomada por autoridad competente en un contexto de concreta amenaza contra la seguridad nacional.

La posterior sentencia del caso G.D. y COMISIONER AN GARDA SÍOCHÁNA, sin embargo, nos advertirá de la imposibilidad de hacer uso de la información así obtenida

[22] Actual art. 61 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

[23] La primera sentencia sería revocada parcialmente por otra de la Gran Sala de 25 de mayo de 2021; la segunda confirmada por otra de la Gran Sala de la misma fecha que la anterior.

más allá del umbral de la protección de la seguridad nacional; de suerte que no podría utilizarse, al menos en una primera impresión del Alto Tribunal, para los fines de una concreta investigación criminal[24].

Pero el más destacado pronunciamiento de la sentencia afectará sin duda a la posibilidad de establecimiento de regímenes de conservación generalizada e indiferenciada de datos, tales y como fueran otrora desdeñados en los precedentes jurisprudenciales y en la propia sentencia del caso LA QUADRATURE DU NET, en un contexto sí de lucha contra la *delincuencia grave,* referentes a *"…las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario"*; y también, en cuanto a la lucha contra la delincuencia y la protección de la seguridad pública, a *"…los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas"*, sin sujeción en este caso a plazo.

Para comprender qué entiende el TJUE por datos de identidad civil hemos de acudir al § 71 de la STJUE del caso G.D. y COMISIONER AN GARDA SÍOCHÁNA. Serían tales aquellos que fueran precisos para poder *"…identificar a las personas que han utilizado tales medios en el contexto de la preparación o la comisión de un acto delictivo grave*". No se trataría, por tanto, de la disponibilidad de información sobre una determinada identidad electrónica; sino que estos datos habrían de facilitar la razón misma por la que se produce la apertura del TJUE: la identificación de la persona física o jurídica que está detrás de una determinada identidad electrónica y, por ende, pudiera serle atribuida el origen o destino de una determinada comunicación objeto de investigación[25] Tales datos deben, en consecuencia, permitir, o al menos facilitar, desvelar la persona física o jurídica que pudiera estar detrás de una determinada comunicación electrónica emitida o recibida; mas no facilitar información sobre ésta. Datos de registro de usuario, de identidad electrónica, de titular o usuario de número de abonado o de punto de terminación de red podrían, por ello, tener cabida en este concepto de datos de identidad civil. Precisamente esta última sentencia, sin duda bajo la inspiración de la STEDH, Secc. 5ª, de 30 de enero de 2020 (caso BREYER v. Alemania; asunto 50001/12), expandiría el elenco de datos susceptibles de esta conservación generalizada e indiscriminada a los datos relacionados con la adquisición de tarjetas de telefonía móvil de prepago. Eso sí, todos estos supuestos habrían de supeditarse a que la regulación nacional garantizara, *"…mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso"*.

De ningún modo deberíamos considerar estos supuestos como listas cerradas. La propia existencia de finalidades diversas que justificaran el reconocimiento de la posibilidad

---

[24] Ciertamente, resulta un tanto artificioso manejar información obtenida por procedimientos de bulk interception para la lucha contra amenazas externas de carácter terrorista; mas no poder utilizar la misma información para perseguir penalmente a los integrantes de la célula terrorista desmantelada gracias a la información obtenida. Es de esperar, por ello, un pronunciamiento ulterior del TJUE que permita la apertura a la utilización de los datos obtenidos cuando exista un cierto grado de homogeneidad entre la finalidad de seguridad nacional que justifica el régimen excepcional y el delito que estuviera detrás de dichas conductas que la ponen en riesgo.

[25] En este sentido, RODRÍGUEZ LAINZ, José Luis., *"La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G.D. y Comissioner an Garda Síochána"*. Diario La Ley, Nº 10058, Sección Tribuna, 28 de abril de 2022, Wolters Kluwer.

legal de legislar sobre la materia podría permitir sin duda la expansión de la nueva doctrina jurisprudencial a otras categorías de datos con las que mostraran afinidad. La razón última del reconocimiento de la posibilidad de conservar datos de asignaciones IP dinámicas se encuentra en que es la única forma de permitir el seguimiento de la trazabilidad de determinadas comunicaciones; por lo que otros identificadores de tránsito similares habrían de poder tener cabida, como pudiera suceder con las asignaciones de IP privadas provistas por prestadores de servicios de Internet a multiplicidad de usuarios bajo una misma IP pública a través de la tecnología CG-NAT[26]. Y si los datos de identidad civil, de los que no serían sino un apéndice los datos de registro de tarjetas de prepago, tienen por finalidad acercarnos a la identidad real de un determinado interlocutor, la apertura a otros datos que permitieran afianzar esta asignación, como pudieran ser datos bancarios o domicilio contractual, referidos como *datos relativos a los abonados* en el art. 18.3 del Convenio Europeo número 185 sobre la Ciberdelincuencia -Convenio de Budapest-[27], no podría ser objeto de un serio cuestionamiento. Y estos son solamente ejemplos, frente a una cambiante tecnología de las comunicaciones electrónicas capaz de variar de forma radical en breves espacios de tiempo su propia arquitectura de funcionamiento.

La conveniencia de la adaptación de nuestra LCDCE a esta jurisprudencia, lejos de la aplicación de un principio de primacía del Derecho de la Unión y de la jurisprudencia que la interpreta -arts. 4 bis de la Ley Orgánica del Poder Judicial y 267 del Tratado de Funcionamiento de la Unión Europea-, es incontestable. Y ello, no tanto en cuanto a la no aplicación de aquello que difícilmente podría sostenerse más allá de una jurisprudencia del Tribunal Supremo tan insistente en tratar de alongar la lenta agonía de la LCDCE al completo, como de homologar aspectos tales como los plazos de conservación de datos y mejor acometer la delimitación del concepto de delito grave que maneja la ley más allá del simple criterio penológico que alberga. Una drástica reducción de los plazos en cuanto incumbe a la conservación de datos relativos a conexiones IP, respecto de los que la jurisprudencia del TJUE ha permitido el establecimiento de regímenes de conservación, aun a sabiendas de la gran capacidad de aportación de información sobre perfiles de los usuarios afectados, sería indispensable; y el concepto de delito grave que maneja aquélla dista mucho de esa concepción penológica que propone la LCDCE; como posteriormente veremos.

B) La retención selectiva de datos: un campo inexplorado en la legislación española

La orden de retención selectiva de datos encuentra por fundamento una decisión adoptada por una autoridad nacional, bajo el control y supervisión de una autoridad judicial o

[26] CG-NAT, acrónimo de *Carrier Grade Network Address Translation,* no es sino una técnica de optimización de las IIPP públicas disponibles para una determinada operadora; mediante la simultánea compartición de una misma IP pública por múltiples usuarios, gracias a la asignación por el operador de IIPP privadas propias. El rastreo de una comunicación canalizada por CG-NAT solo permitiría identificar al volumen de usuarios que estuvieran conectados a la vez con una misma IP pública, más no al que hubiera emitido o una determinada comunicación. La conservación de la asignación de estas IIPP privadas por tiempos limitados podría ser crucial para el éxito de investigaciones criminales.

[27] Hemos preferido no hacer referencia a los nuevos procedimientos de obtención de evidencias electrónicas contenidos en el Segundo Protocolo Adicional al Convenio Europeo sobre la Ciberdelincuencia, relativo a la cooperación reforzada y revelación de pruebas electrónicas; como norma que no cuenta aún con su ratificación por el Estado español.

administrativa independiente, por virtud de la cual se ordena a determinados prestadores de servicios de comunicaciones electrónicas la retención de determinados datos relativos a comunicaciones en base a criterios definitorios de su concreto alcance. Estos criterios pueden ser subjetivos, temporales, espaciales, teleológicos o resultado de la conjunción de unos y otros.

La gran diferencia que la aparta del ejemplo de la conservación preventiva e indiscriminada de datos que regulara la Directiva 2006/24/CE radica en que, sin perjuicio de la existencia de una previa norma habilitante que da cobertura legal a la injerencia, el mecanismo de conservación se activa no ope legis, sino como consecuencia de una concreta decisión dictada por autoridad competente y para una finalidad concreta, generalmente relacionada con la seguridad nacional, la seguridad pública o la prevención de la delincuencia. Pongamos un ejemplo: Una cumbre de Ministros de Defensa de la OTAN decide reunirse durante una semana en la localidad de Trier; la autoridad gubernativa decide ordenar la retención de los datos de tráfico y geolocalización en un radio de cinco kilómetros de la sede del encuentro como forma de prevenir la presencia de elementos terroristas y eventuales atentados. Si hablamos de una decisión de una autoridad encargada de la investigación de infracciones en el curso de un procedimiento de investigación criminal nos enfrentaríamos ante una realidad diversa: una orden interceptación de los mismos datos en tiempo real, dirigida precisamente al esclarecimiento de los hechos que son objeto de investigación. La retención de datos, aunque pueda coincidir en el mismo objetivo de lucha contra la delincuencia, está diseñada siempre desde una perspectiva preventiva[28]; mientras que la orden de interceptación de datos en tiempo real tiene por objetivo específico la obtención de evidencias o fuentes de conocimiento en el curso de una concreta investigación criminal.

La STJUE del caso TELE2 SVERIGE AB y otros[29] ya adelantó la conformidad con el art. 15.1 de la Directiva 2002/58/CE de esta herramienta de injerencia; estableciendo los primeros criterios definitorios de los márgenes de conformidad con el Derecho de la Unión de dichas técnicas. Pero habríamos de esperar sin duda a la sentencia del caso LA QUADRATURE DU NET y otros para encontrar una más perfecta definición y delimitación jurídica de tal técnica de injerencia. En el fallo de esta sentencia podemos encontrar efectivamente el siguiente pronunciamiento: serían conformes al Derecho de la Unión medidas legislativas *"…que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la*

[28] Pongamos otro ejemplo: Hay constancia de que en un determinado barrio de ciudad costera hay un altísimo índice de operaciones de desembarco de alijos de drogas y ulterior ocultación en viviendas o habitáculos a disposición de residentes. La autoridad gubernativa, que detecta en un período de tiempo determinado un incremento en el movimiento sospechoso de lanchas o *gomas*, decide emitir orden de retención de datos de tráfico y geolocalización, coincidiendo con ese período de mayor incidencia, aún sin dirigir la investigación contra personas concretas. La sentencia comentada, en su § 150 ponía como ejemplos de delimitación geográfica en el contexto de la lucha contra la delincuencia a *"…lugares que cuentan con un número elevado de delitos graves, lugares especialmente expuestos a la comisión de delitos graves, como los lugares o infraestructuras a los que acuden con regularidad un número muy elevado de personas, o incluso lugares estratégicos, como aeropuertos, estaciones o zonas de peajes".*

[29] ORTIZ PRADILLO, Juan Carlos: *"Europa: Auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas"* (Revista General de Derecho Procesal 52 (2020), realiza un interesante comentario a la sentencia y posibilidad de aplicación de estos regímenes de conservación selectiva de datos en el ordenamiento jurídico español.

base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse".

El ordenamiento jurídico español, aún anclado en la agónica pervivencia de nuestra LCDCE, no cuenta con ningún referente normativo que pudiera aprovechar esta puerta abierta ofrecida por la jurisprudencia del Tribunal de Luxemburgo. Sin embargo, sería sin duda una excelente solución capaz de copar parte del vacío normativo que habría de surgir una vez que la doctrina del TJUE sobre los regímenes de conservación preventiva e indiscriminada de datos a los efectos de eventuales ulteriores investigaciones criminales termine de imponerse.

C) Deberes legales de preservación y cesión de datos en relación con contenidos ilícitos en las redes de comunicaciones

El Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo de 29 de abril de 2021 sobre la lucha contra la difusión de contenidos terroristas en línea ha inaugurado un cuerpo normativo de la Unión destinado a proteger las redes contra el alojamiento y difusión de determinados contenidos ilícitos en el ámbito de los servicios ofrecidos por prestadores de servicios de alojamiento de datos. El esquema de la norma partía de la imposición de un especial deber de diligencia que imponía a éstos, cuando estuvieran expuestos a contenidos terroristas, en los términos descritos en el art. 4 del Reglamento, una actitud vigilante, con respeto de elementales criterios de proporcionalidad y no discriminación; que les llevaría por una parte a poner en conocimiento a las autoridades competentes la existencia de contenidos terroristas, y, por otra, al borrado y bloqueo inmediato de éstos como consecuencia de una orden remitida por autoridad competente. Este deber, nos dirá su art. 5.2, habría de garantizar la adopción de las medidas adecuadas para *"…identificar y retirar los contenidos terroristas o bloquear el acceso a ellos rápidamente"*. Este deber habría de ir acompañado, tanto en el supuesto de que se hubiera recibido una orden concreta, como por razón de la *gravedad del nivel exposición*[30], de la obligación de conservar datos de contenido, y especialmente los relacionados con la trazabilidad del origen de tales contenidos, *datos anexos* -art. 6-; que se prolongará por un plazo de seis meses ampliable.

Inmediatamente a esta norma comunitaria le siguió el Reglamento (UE) 2021/1232[31]. La norma, temerosa sin duda de una posible reacción desfavorable del TJUE, nacida inicialmente con una vocación temporal, seguirá una misma línea de imposición a determinados operadores, los proveedores de servicios de comunicaciones interpersonales independientes de la numeración[32], del deber de adopción de determinadas medidas proactivas en búsqueda de contenidos en línea relacionados con la pornografía infantil o la explotación se-

[30] El concepto de exposición a contenidos terroristas, del que se deriva un haz de obligaciones de prevención y diligencia, viene recogido en el art. 5.4 del Reglamento.

[31] Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo de 14 de julio de 2021 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea.

[32] El 2.7 de la Directiva (UE) 2018/1972 define a éstos como *"servicio de comunicaciones interpersonales que no conecta a través de recursos de numeración pública asignados, es decir, de un número o números de los planes de numeración nacional o internacional, o no permite la comunicación con un número o números de los planes de numeración nacional o internacional".*

xual de menores en las redes. Se huirá aquí de ese concepto de exposición manejado por el Reglamento (UE) 2021/784, para imponerse a todos los operadores concernidos, independientemente de la previa constatación o no de tales contenidos en las bases de datos por ellos gestionadas. No nos interesa en este caso una referencia al *hashing* como técnica de prospección automática que propone el Reglamento, como el deber que se impone a los operadores concernidos, como consecuencia de la detección de un contenido sospechoso de albergar pornografía infantil, una vez comprobado de forma individualizada tal realidad, proceder a su denuncia a la autoridad competente o entidad asociativa dedicada a la lucha contra los abusos sexuales contra menores; así como a retener esta información a las resultas de una posible utilización en el contexto de una eventual ulterior investigación criminal. El apartado i) del art. 3.1 es la norma que sujeta la medida a estrictos límites temporales: los datos asociados relacionados con tales contenidos ilícitos detectados no podrán almacenarse *"…más tiempo del estrictamente necesario para el fin pertinente establecido en la letra h) y, en cualquier caso, no más de doce meses a partir de la fecha en que se detectó el presunto abuso sexual de menores en línea"* [33]. Este plazo, obviamente, habrá de prolongarse a merced de la decisión que adopte la autoridad competente para la investigación del hecho, una vez que se haya emitido la correspondiente orden de cesión, y en los términos y bajo las condiciones que impongan la orden y la norma habilitante del correspondiente Estado miembro de la unión.

Esta línea principiada por el Reglamento (UE) 2021/784 ha encontrado un nuevo reflejo en el Reglamento (UE) 2022/2065, conocido como Reglamento de Servicios Digitales[34]. El Reglamento, en cierto modo, expande esos deberes de participación proactiva que se impusiera a los prestadores de servicios de alojamiento concernidos por el mandato del Reglamento (UE) 2021/784, generalizándolos en la lucha contra determinados contenidos ilícitos. Aunque aquí tampoco se impondrán deberes de empleo de técnicas de hashing en la detección de tales contenidos[35], como sucediera con los referidos a la pornografía infantil o explotación sexual de menores, el conocimiento, o sospecha, de que se ha cometido, se está cometiendo o puede que se cometa *"…un delito que implique una amenaza para la vida o la seguridad de una o más personas"* genera en el operador de servicios de alojamiento de datos concernido, por mandato de su art. 18.1, un concreto deber de comunicar de inmediato tal circunstancia a las autoridades policiales o judiciales del Estado miembro afectado; con obligación de aportar

[33] El apartado v) del mismo art. 3.1 impone a los prestadores el deber de proporcionar a las autoridades competentes *"…los datos necesarios para la prevención, detección, investigación o enjuiciamiento de infracciones penales establecidas en la Directiva 2011/93/UE"*; lo que habrá de incluir sin duda a los datos de tráfico e identitarios que se posean y permitan avanzar en la trazabilidad del origen de la información compartida y posibles destinatarios.

[34] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

[35] El empleo de *medios automatizados* como política basada en la que se define como *declaración de motivos*, no se descarta, sin embargo, de raíz. EL art. 17.3, en su apartado b) reconoce, además de los canales de denuncia, la iniciativa propia del prestador para la indagación de contenidos ilícitos; mientras que el apartado c) hace mención a la posibilidad de empleo de *medios automatizados* para la detección o identificación de contenidos ilícitos. Todo se hace depender de la inserción de estas facultades que se atribuye el prestador en la declaración de motivos disponible para todos los usuarios que pretendan acceder a los servicios que ponga a su disposición el prestador de servicios de alojamiento.

igualmente *toda la información pertinente de que disponga*[36]. La norma, sin embargo, no prevé ningún mecanismo de almacenamiento o conservación del contenido ilícito detectado; pero ello es una consecuencia necesaria del mismo hecho de la denuncia. Debería, por tanto, conservar esa información al menos hasta que se reciba un pronunciamiento específico de la autoridad nacional competente sobre el destino que ha de darse a tales contenidos y datos asociados.

Como podemos comprobar en estos tres casos, independientemente de los deberes de involucración que se imponen a los distintos sujetos obligados, el deber de cesión y conservación de datos que impone o presupone la norma comunitaria se hace depender de un criterio selectivo basado en la detección y comprobación de existencia de determinados contenidos ilícitos; y es en base a esta constatación cuando surge una obligación de conservación que, realmente, es gregaria de la disponibilidad de la información precisa al objeto de poder ser utilizada como evidencia, una vez que la autoridad nacional competente tome una decisión sobre el inicio de una investigación criminal. El deber de conservación surge, por tanto, del cumplimiento por el prestador de un deber de denuncia; y con la finalidad de preservar la información sobre contenidos, identidad electrónica responsable y trazabilidad de los mismos a los efectos de tal investigación criminal.

Los dos primeros Reglamentos se encuentran actualmente en vigor, por lo que pueden ser de plena aplicación en nuestro ordenamiento jurídico interno; el tercero habrá de esperar hasta el 17 de febrero de 2024.

D) Órdenes de preservación rápida de datos relativos a las comunicaciones: Las *quick freezing orders*

El origen de las órdenes de preservación de datos ha de encontrarse sin duda en el art. 16 del Convenio de Budapest. Estas surgen realmente como consecuencia de la necesidad de garantizar la preservación de información que podría destruirse antes de que se diera respuesta a una determinada solicitud de cooperación judicial internacional de cesión de datos por los cauces ordinarios. Se agilizan los trámites y se desformaliza el empleo de los mecanismos tradicionales de cooperación precisamente para garantizar una retención de datos que no garantizaba en ese primer momento que la cesión llegara a buen fin. El legislador español, en su art. 588 octies de la LECRIM, se inspira en dicha norma, tal y como reconoce en el Preámbulo de la Ley Orgánica 13/2015; aunque realmente lo importa a un esquema en el que la postergación de la intervención decisoria de la autoridad judicial no encuentra precisamente un encaje sencillo con la doctrina del TJUE, como posteriormente podremos apreciar.

[36] La norma debe ser complementada con la posibilidad de cesión de datos por parte de entidades privadas o particulares a EUROPOL a que hacen referencia los arts. 17, 18, 26.2 y 27 del Reglamento (UE) 2016/794 (Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo), recientemente modificado por el Reglamento (UE) 2022/991 (Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo de 8 de junio de 2022 por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación); especialmente en materia de lucha contra la difusión en línea de abusos sexuales a menores -art. 26 ter-, o de *situaciones de crisis en línea.*

Este esquema de preservación supone una conservación de decisión instantánea, selectiva e individualizada según parámetros que nos recuerdan claramente la propia estructura y naturaleza de las técnicas de retención selectiva de datos a la que antes hemos hecho referencia. Lo único que hace realmente que difiera de éstas es, por una parte, la urgencia en su decisión, soliendo dar lugar a que sea una autoridad policial, administrativa o fiscal quien la acuerde, a reserva de una ulterior decisión de autoridad judicial o administrativa independiente; y, por otra, que el criterio de selección camina precisamente hacia la mayor individualización posible, forzada por un determinado acontecimiento que exige la inmediata preservación de unos datos de conservación marcadamente fugaz, y a las resultas de una concreta actuación investigadora. El ejemplo más evidente de ello podría ser el de ordenar que se conserven los datos de geolocalización gestionados por una determinada estación BTS en cuyo radio de acción acabara de cometerse un asesinato.

La STJUE del caso LA QUADRATURE DU NET y otros vuelve a ser el referente para el reconocimiento de este tipo de medidas de investigación, con las mismas condiciones que los restantes ejemplos que abarca en relación a la existencia de adecuadas normas materiales y procesales y despliegue de garantías contra los riesgos de abuso. Efectivamente, la conformidad del art. 15.1 de la Directiva 2002/58/CE, y en cuanto a la lucha contra la delincuencia grave y la protección de la seguridad nacional, lo sería a la posibilidad de *"…recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan estos proveedores de servicios"*.

Los datos de tráfico y localización a los que puede accederse por esta técnica no son otros que aquéllos que los operadores concernidos pueden conservar con motivo de la prestación del servicio de comunicaciones electrónicas, durante los plazos que habrían de determinarse por las normas de desarrollo de la Directiva 2002/58/CE; nos dirá la sentencia en su § 160. Por ello, realmente esta herramienta asume el cometido de que esos datos no pasen a ser destruidos o convertidos en anónimos, una vez perdida su funcionalidad. Y como consecuencia de que lo que se pretende es dar a dichos datos un destino diverso al propio para el que fueran objeto de almacenamiento y tratamiento, la sentencia impondrá, aparte de plazos razonables de conservación, por una parte, la necesidad de un control jurisdiccional efectivo, independientemente de la autoridad competente para la toma de decisión; y, por otra, un mayor rigor en la determinación del criterio de superación del juicio de proporcionalidad, a la hora de definir las infracciones criminales cuya investigación puede permitir el uso de esta herramienta: la lucha contra la delincuencia grave. Se impone, igualmente, un deber de máxima restricción a la hora de seleccionar los datos que han de ser objeto de preservación. Por ello, nos dirá el § 164 que: *"Además, para garantizar que la injerencia que supone una medida de este tipo se limite a lo estrictamente necesario, es preciso, por una parte, que la obligación de conservación ataña únicamente a los datos de tráfico y de localización que puedan contribuir a la investigación del delito grave o del atentado a la seguridad nacional de que se trate. Por otra parte, la duración de conservación de los datos debe limitarse a lo estrictamente necesario, si bien podrá ampliarse cuando las circunstancias y el objetivo perseguido por dicha medida lo justifiquen"*.

Sin embargo, el TJUE es comprensivo a la hora de delimitar el alcance subjetivo de este tipo de medidas, en las que la intuición y la necesidad perentoria de afianzar la preservación de datos sobre los que poder articular una investigación criminal en un primer momento en que las incertidumbres impiden atribuir a persona concreta la cualidad de sospechosa. Se

permitirá, por ello -§165- recabar información respecto de personas no sospechosas de haber planeado o cometido un delito grave, en tanto en cuanto los datos de tráfico o de localización cuya preservación se ordena, puedan, *"…sobre la base de elementos objetivos y no discriminatorios, contribuir a la investigación de dicho delito"*[37].

Por último, ese criterio de subsidiariedad o conexión respecto de la información que pretende obtenerse, del mecanismo de cesión de datos que pretenda emplearse una vez garantizada la preservación, aunque pareciera no ser tenido en cuenta en el §164, al dotar de cierta autonomía a la exigencia propia de delincuencia grave que delimita su finalidad, quedará claramente definido en el parágrafo siguiente: la orden de preservación de datos, aunque por sí misma constituiría una grave inmisión sobre derechos del entorno de la privacidad de las personas afectadas merecedora de ese elevado estándar de protección que impone el TJUE, no tiene sentido si no se relaciona con los requisitos impuestos para la utilidad que pretende darse a la información retenida. En otras palabras: *"El acceso de las autoridades competentes a los datos conservados de este modo debe efectuarse respetando los requisitos que se derivan de la jurisprudencia que ha interpretado la Directiva 2002/58"*.

La comparativa de esta previsión de la sentencia del caso LA QUADRATURE DU NET y otros con nuestro actual art. 588 octies de la LECRIM no puede resultar más preocupante. La norma, que va más allá en su enunciado de la simple preservación de datos de tráfico y localización (*datos o informaciones concretas incluidas en un sistema informático de almacenamiento*), parte de una comprometida disociación entre la decisión de la autoridad policial o fiscal que le sirve de fundamento y el ulterior control judicial. Con la idea de que fuera en el ulterior momento de la emisión de la oportuna orden de cesión de todos o parte de los datos cuya retención se ha ordenado cuando la medida sería sometida a un efectivo control judicial (el juez de instrucción puede limitarse no solo a controlar la viabilidad jurídica de la solicitud de cesión de concretos datos de entre los preservados, sino también valorar la conformidad a derecho de la decisión de preservación misma), lo cierto es que, lege data, solamente se someterían a control judicial tales decisiones en tanto que se decidiera finalmente acudir al juez para que se emitiera la orden de cesión. A *contrario sensu*, en aquellos supuestos en que la investigación no fructificara, las órdenes de preservación quedarían hueras de cualquier tipo de control judicial. Realmente, la exagerada laxitud de los plazos de vigencia de la medida (hasta 180 días) confirma la sospecha de que el legislador ha diseñado una herramienta en la que el control judicial solamente se reservaría para los supuestos en los que una orden de cesión de datos es finalmente objeto de solicitud, en base a la previa orden de preservación. El riesgo de abuso o arbitrariedad, cuya evitación inspira sin duda al Tribunal de Luxemburgo, difícilmente podría soslayarse con tal redacción y estructura del art. 588 octies de la LECRIM.

Habría bastado con convertir la medida en una herramienta de anticipación de autorización judicial específica de preservación de datos, necesitada de una ratificación en un plazo perentorio, para que la norma nacional, aparte de sujetarse a la exigencia de superación del

[37] El referido parágrafo pone como ejemplos los datos de la víctima del delito, de su entorno social o profesional, o incluso de zonas geográficas determinadas, como los lugares en que se cometió y se preparó el delito o el atentado contra la seguridad nacional de que se trate. La preservación de datos generados en torno a una estación BTS, que tanta trascendencia podría tener para la selección o confirmación de personas sospechosas de la comisión de un delito de especial gravedad en una franja de tiempo perfectamente definida, podría, por tanto, tener cabida en el mandato del art. 15.1 de la Directiva 2002/58/CE; obviamente con la adopción de las debidas cautelas y prevenciones en orden a su ulterior utilización y análisis.

concepto de delito grave, sí asociado a la naturaleza de la medida de cesión de datos de tráfico o de localización derivada de aquélla[38], superara las exigencias de la jurisprudencia del TJUE.

Entre tanto pudiera procederse a una conveniente reforma del precepto, se hacía preciso articular un mecanismo de comunicación a la autoridad judicial del hecho de la decisión adoptada por autoridad policial o fiscal, como forma de someter ésta a un control judicial efectivo como el requerido por dicha jurisprudencia. La puesta en conocimiento del inicio de actuaciones de investigación en base a lo establecido el art. 284.1 de la LECRIM podría servir de base legal para esta interpretación de la norma conforme con el mandato de la STJUE del caso LA QUADRATURE DU NET y otros; mientras que el apartado segundo del mismo precepto, en cuanto que da lugar a la no remisión del atestado ante el no descubrimiento de la identidad del autor, podría reinterpretarse en el sentido de permitirla cuando se hubieran adoptado medidas afectantes a concretos derechos fundamentales en base a alguna de las medidas de investigación tecnológicas que la LECRIM exime de previa autorización judicial[39]. Igual podría suceder en aplicación del mandato del art. 5.3 de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal; abriendo la norma a la posibilidad de puesta en conocimiento de aquellas investigaciones preprocesales en que se hubiera ordenado una medida de preservación rápida de datos.

Esta posibilidad de forzamiento de la interpretación de las normas citadas para favorecer en todo caso la puesta en conocimiento de la decisión adoptada por una autoridad fiscal o policial de preservación de datos se ha convertido en obligación tras la entrada en vigor de la LO 7/2021[40]; cuyo art. 7.1 sí impone este deber de dación de cuenta a la autoridad judicial, cuando se hubiera emitido una orden de cesión de datos. Es evidente que la preservación podría no entenderse en sí misma como una cesión sometida al mandato de dicho precepto, al ser previa a una petición de cesión de datos. Pero hemos de partir de la premisa de que la preservación no sería sino la antesala de una posible petición de cesión de datos, que nos llevaría a la posibilidad de equipararla en sí misma a un tratamiento de datos personales; y el art. 3.2 de la Directiva (UE) 2016/680 incluye dentro del concepto de tratamiento a cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, entre las que se encontraría su mera conservación. Este deber de dación de cuenta no es en sí mismo una vía para garantizar la ra-

---

[38] En este sentido: RODRÍGUEZ LAINZ, José Luis., *"Necesidades de reconsideración o reforma de la normativa procesal sobre medidas de investigación tecnológica"*; en: *Blockchain, inteligencia artificial y criptomonedas en el proceso penal.* Colección: Cuadernos Digitales de Formación Nº volumen: 12 Año: 2022. CGPJ.

[39] La norma no prohíbe, sino que exime del deber de poner en conocimiento de la autoridad judicial los atestados sin autor conocido no relacionados en el mismo precepto. Bastaría con una orden general o instrucción emitida en el seno del Ministerio del Interior, o incluso de la Fiscalía General del Estado, para que se impusiera esta rutina de remisión, que permitiera un control efectivo por la autoridad judicial de la procedencia y conformidad a derecho de la medida de preservación de datos acordada. De hecho, el art. 284.2,c) de la LECRIM permite la remisión de atestados por decisión de la autoridad fiscal; aunque aparente referirse a actuaciones concretas. La práctica judicial cotidiana está experimentando, con posible fundamento en el art. 284.2,b) de la LECRIM, la remisión rutinaria a la autoridad judicial de atestados con resultado fallido, en los que se han emitido por la policía judicial órdenes de cesión de datos del tipo identidades electrónicas o datos financieros o bancarios.

[40] Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

tificación judicial de la medida en aquellos supuestos en que no se solicitara una concreta orden de cesión de datos; pero al menos abre las puertas para su sometimiento a un efectivo control externo, aunque necesitado, al igual que en el supuesto del art. 588 ter m de la LECRIM, de una regulación concreta que le dé forma y contenido.

IV) LA CESIÓN DE DATOS COMERCIALES EN EL CONTEXTO DE UNA INVESTIGACIÓN CRIMINAL EN LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Una vez establecidas las diferencias con otras posibles herramientas o fuentes de obtención de datos gestionados por las operadoras de comunicaciones que encuentran su respaldo en la interpretación por el TJUE del art. 15.1 de la Directiva, podemos enfrentarnos al reto de determinar si es factible que, en el curso de una investigación criminal, puedan recabarse datos de tráfico o de localización que estuvieran siendo objeto de almacenamiento y tratamiento por los prestadores de servicios sometidos al mandato de la Directiva 2022/58/CE; tipologías de delitos susceptibles de dar lugar a una orden de cesión legítima, así como exigencias formales y materiales en orden a la tramitación de la orden.

Realmente, podremos comprobar cómo el escenario llegará a variar en parte frente a los ejemplos anteriormente analizados; toda vez que el tratamiento de la información objeto de cesión, tal y como sucediera respecto de las órdenes de preservación rápida de datos, excede de las finalidades concretas que legitiman a las operadoras para llevar a efecto el tratamiento. Por ello adquirirán tanta trascendencia la definición y aplicación de las normas sobre excepciones a los principios del consentimiento y finalidad en la protección de datos personales recogidas en el RGPD, y su aplicación al ámbito de su utilización con motivo de salvaguardia de determinados fines públicos, entre los que se encuentra la lucha contra la delincuencia en la Directiva (UE) 2016/680; los cuales han jugado un especial papel tanto en la reciente STJUE (Sala Sexta) de 17 de noviembre de 2022 (caso SPETSIALIZIRAN NAKAZATELEN SAD; asunto C-350/21)[41], como en la STS 824/2022, de 19 de octubre.

A) Breve referencia a los datos que pueden ser conservados por motivos comerciales por los operadores de comunicaciones electrónicas y proveedores de servicios de Internet equiparables

La tantas veces citada STJUE del caso LA QUADRATURE DU NET y otros hacía mención expresa a que serían las normas internas de los Estados miembros las que habría de definir qué datos de entre los tratados por los prestadores de servicios de comunicaciones electrónicas podían someterse a las excepciones contenidas en los arts. 6 y 9 de la Directiva 2002/58/CE; en cuanto que sometidas a ese criterio de funcionalidad que justificaría precisamente su tratamiento. Tal legitimidad se convertiría sin duda en presupuesto para la ulterior emisión de órdenes de cesión de datos por la autoridad competente sin perjuicio de que la misma fuente, aún ilícita, pudiera servir de evidencia o fuente de conocimiento en investigaciones criminales, cuando se dieran las circunstancias precisas para su admisibilidad como tal.

A nivel nacional, el ya derogado Real Decreto 1736/1998, de 31 de julio[42], discri-

[41] Trabajaremos una traducción propia al castellano de la versión oficial en francés; toda vez que al día de la fecha aún no se ha publicado en la web oficial del TJUE la traducción a otras lenguas que al búlgaro y al francés.

[42] Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el Título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunica-

minaba en su art. 65 con cierta claridad entre lo que era el tratamiento de datos de tráfico que debían ser usados para el establecimiento de una comunicación, sometidos a un régimen de destrucción o conversión en anónimos una vez desaparecida tal funcionalidad, y aquéllos que podían ser tratados *exclusivamente con el objeto de realizar la facturación y los pagos de las interconexiones*. Estos datos que podían ser objeto de conservación a tal efecto aparecían descritos en el apartado 2 de dicho precepto: Número de identificación del abonado; dirección del abonado y tipo de equipo terminal empleado para las llamadas; número total de unidades que deben facturarse durante el ejercicio contable; número de abonado que recibe la llamada; tipo, hora de comienzo y duración de las llamadas o volumen de datos transmitiros; fecha de la llamada o del servicio, así como otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes.

Dicho reglamento sería derogado por el ya referenciado RD 424/2005 que no llegaría a contener un precepto de similar o equivalente contenido, derivándose las normas sobre protección de consumidores en materia de sus datos personales al nuevo RD 899/2009, cuyo art. 31 se remitía a su vez a lo establecido en la entonces vigente LGT y el RD 424/2005. Sin embargo, desde el punto de vista de la limitación en el tratamiento de datos por parte de las operadoras de comunicaciones electrónicas, este concepto de datos relativos a las comunicaciones que manejara el reglamento de 1998 nos podría acercar a una representación importante de estos datos de tráfico en los que podemos apreciar con claridad cómo pueden diferenciarse unos que sí atienden a la prestación de un determinado servicio de comunicaciones demandado por el usuario (coincidentes en buena parte con los descritos por la STEDH del caso MALONE v. Reino Unido: Existencia, origen y destino, datación, tipo de comunicación, duración y/o volumen de carga de transferencia); frente a otros que se corresponderían con una dimensión estática, y cuyo cometido no sería otro que el de poder identificar a la persona que emite o recibe la comunicación: datos de identidad civil.

Pero esta definición no atendería sino a las tradicionales comunicaciones electrónicas; no al intercambio de información a través de los denominados *servicios de comunicaciones interpersonales independientes de la numeración*, o servicios de comunicaciones vía Internet (mensajería instantánea, VoIP, chats privados de redes sociales, videoconferencias…), ni a aquellos datos que se generan y tratan para garantizar la conectividad de los servicios de comunicaciones que los distintos prestadores ofrecen a sus usuarios.

Precisamente en el campo del dato de tráfico que debe ser tratado para la canalización de concretas comunicaciones, y no tanto en el de la facturación al que hiciera específica referencia el art. 65.2 del RD 1736/1998, es donde podrían surgir más dudas en cuanto a su verdadero alcance. El art. 1.d) del Convenio de Budapest recogerá un concepto extenso de datos de tráfico; pero que se quedará precisamente en ese estrecho horizonte que representa la concreta conducción de una comunicación. Serían datos de tráfico: *"cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente".*

Sin embargo, para encontrar una norma que permita establecer una relación de unos datos íntimamente ligados a éstos y que participan del mismo cometido de garantizar la con-

ciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones.

ducción de comunicaciones, aunque sin formar parte directa de éstas, los datos de conectividad, habríamos de acudir a una norma nacional: el art. 588 ter b, párrafo tercero, de la LECRIM: "*A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga*". Ello no significa, sin embargo, que esa equiparación a efectos de la investigación criminal desvirtúe su naturaleza jurídica plenamente diferenciable del dato de tráfico, cuya dimensión dinámica se encuentra protegida por la fuerte protección de barrera anticipada que supone el derecho al secreto de las comunicaciones.

Sobre todo, en el universo de Internet, definir correctamente unos concretos datos manejados por el prestador como datos de tráfico y no simplemente como identitarios o de autentificación del usuario, no es precisamente una tarea fácil; y menos comprender que la conservación de alguno de ellos por la operadora correspondiente se convierte en clave esencial para la prestación del servicio. Pero incluso en el mundo de la telefonía móvil, bajo tecnología GSM, nos enfrentamos a complejos dilemas jurídicos.

Desde el punto de vista de la telefonía móvil, es indiscutible que los identificadores IMEI e IMSI y la asociación entre ambos[43] son datos estáticos que se encuadran fácilmente en el ámbito de la identidad civil por lo que, cuando son extraídos mediante la técnica conocida como IMSI cátcher[44], ni siquiera podrían concebirse como genuinos datos de conectividad. Sin embargo, y sin necesidad del previo establecimiento o recepción de una comunicación, cuando el terminal entra en contacto con una estación BTS compartirá de forma permanente, aunque no constante, información sobre su localización con ésta a través del conocido como *canal de control* –RACH-. Su cometido es poder tener localizado en todo momento al terminal a los efectos de canalizar cualquier comunicación que al mismo fuera dirigida; y con ella podría establecerse una lista de todos los dispositivos que hubieran estado bajo el campo de influencia de una determinada estación en un período de tiempo determinado. No es el dato generado en sí un dato de localización, aunque permite la localización del terminal con cierto grado de precisión; especialmente si lo relacionamos con otras estaciones BTS con las que se hubiera establecido contacto[45]. Pero lo que más nos interesa en este sentido es que tal dato de conectividad habrá de ser objeto de tratamiento por la operadora, cuando menos, durante el tiempo en que se mantenga la relación del dispositivo con la estación BTS de referencia. Por otra parte, cuando un terminal procede a la desconexión convencional o apagado del dispositivo, el *canal dedicado* que entre los canales de difusión atiende en concreto al dispositivo

[43] La activación de una tarjeta SIM en un dispositivo móvil genera una asociación entre el número de IMSI de ésta y la numeración IMEI que identifica al dispositivo físico. Esta interconexión da paso a un protocolo de autenticación cuya finalidad es la de reconocerla como íntimamente unida al número de abonado que soporta la tarjeta SIM; siendo esta información conservada por la correspondiente operadora a través de bases de datos conocidas como HLR -*home location register*-. A partir de este momento, cualquier petición de comunicación con determinado terminal telefónico se realiza a través del número de abonado; traduciéndose vía estas bases de datos en la asociación IMEI/IMSI registrada.

[44] Véase como último ejemplo jurisprudencial de una larga lista de precedentes que estuvieran detrás de la redacción del actual art. 588 ter l la reciente STS 199/2023, de 21 de marzo.

[45] Aunque se mantenga el ligamen con la estación BTS de referencia, las estaciones de telefonía móvil en el área de influencia del terminal intentarán contactar con éste mediante la emisión de señales de balizamiento emitidas a través de los conocidos como *canales de difusión* –BCCH-; generando datos relativos a tal interconexión.

comenzará a emitir por períodos regulares y por un tiempo de hasta 72 horas señales tendentes a recuperar la conexión con el terminal y que permitirán mantener viva la información sobre la interconexión entre terminal y estación. Es fácil comprobar cómo tales combinaciones de procedimientos automáticos llegan a desdibujar incluso la propia naturaleza del dato. Sin embargo, cuando emitimos una comunicación la información sobre nuestro IMEI/IMSI se convierte a su vez en un dato de tráfico que es enviado al prestador del servicio de telefonía contratado para su gestión.

La transmisión de datos vía Internet nos enfrenta igualmente a similares dilemas, al entrar en acción unos mismos datos que pudieran ser meros identificadores identitarios; como son el punto de conexión de red del *router -acces point* o *AP*- con el que conectamos y la MAC o identificativo individualizado de la tarjeta de red del dispositivo de comunicación a aquél conectado y la asociación de ambos a través de una IP privada. Al realizarse la conexión por Internet da comienzo de un complicado proceso de detección, autenticación y obtención de permisos, a través de los llamados *paquetes de administración.* Pero una vez sellada esta asociación toda esta información formará parte de aquello que se transmite, como dato de tráfico; haciéndose visible a través de las llamadas *cabeceras IP -IP headers*- de los paquetes de datos. En tanto en cuanto el dispositivo permanezca conectado a la red, bien mediante la asignación de una IP dinámica exclusiva, bien mediante la compartición de ésta con una IP privada gestionada a través de una IP común en un sistema de CG-NAT, la operadora que esté prestando el correspondiente servicio de acceso a Internet deberá poder conservar y tratar dichos datos y ello independientemente del alcance del consentimiento de quien haya aceptado las condiciones de uso del proveedor, y de la legislación más o menos estricta a la que se sujete éste en su funcionamiento. Pero es que igualmente surgirá un interés legítimo en conservar la misma asignación de la IP dinámica a un determinado usuario; toda vez que, pese al número finito y limitado de IIPP que gestiona cada operadora, necesidades operativas hacen muy conveniente mantener en la medida de lo posible una misma asignación a cada punto de terminación de red al menos cuando se trate de conexión vía punto de terminación de red, no de navegación mediante datos.

La STS 551/2016, de 22 de junio, se enfrentó al difícil reto de analizar la naturaleza jurídica del acceso a información sobre la clave PIN del sistema operativo *OS Blackberry*, como componente de la estructura de funcionamiento de la aplicación de mensajería instantánea conocida como *Blackberry Messages* –BBM-. La clave PIN, al igual que sucede con la clave de usuario de dispositivos tipo iPhone, se comporta como auténtico dato autenticador del usuario; capaces ambos de ofrecer una vigorosa protección de la información contenida en los dispositivos mediante protocolos de encriptación. Pero, aunque la mencionada sentencia no se atrevió a ir más allá de atribuirle una significación de dato identitario perfectamente equiparable al IMSI o IMEI de un terminal telefónico, lo cierto es que este dato asume el importantísimo cometido no solo de permitir a quien lo introduce emitir una determinada comunicación de mensajería instantánea, autenticando su origen, sino también de ser clave para permitir el proceso de encriptación/desencriptación del mensaje en su tránsito hacia su destinatario. De hecho, este dato circula encriptado en la cabecera IP del paquete de datos que se emite; por lo que su consideración como dato de tráfico sería indiscutible.

Si la lógica propia de la facturación de la telefonía móvil o fija permite la conservación de estos datos para una concreta finalidad comercial, podremos encontrar, por último, una justificación razonable, en cuanto respecta cuando menos a datos de tráfico de mensajería instantánea del tipo Outlook o Gmail, o chats privados asociados a determinadas redes sociales: La información puede permanecer a disposición del usuario, y bajo en control del presta-

dor del servicio, alojada en bases de datos propias de éste[46], cuando menos hasta que el usuario proceda a su definitivo borrado o eliminación. Y ello permitiría igualmente, dependiendo del esquema de funcionamiento de la aplicación, que la operadora pueda tener acceso a dicha información conservada como acreditación del tráfico de comunicaciones de determinado usuario durante un tiempo indefinido que solo de éste dependerá.

En definitiva, establecer indiscutibles categorías de datos relativos a comunicaciones que pueden ser conservados por las operadoras por alguno de los motivos referenciados en el art. 6 de la Directiva 2002/58/CE, o datos de conectividad que pudieran relacionarse con éstos, resulta una empresa arriesgada que exigirá una ponderada valoración de la forma y momento de captación o generación del dato. La diferencia entre datos relacionados con la identidad civil, física o jurídica, que está detrás de una determinada persona, o con el tránsito de una determinada comunicación o la geolocalización del dispositivo en el momento de su emisión o recepción por el destinatario, sin embargo, habrá de ser crucial a la hora de determinar la ponderación de principios rectores de trascendencia constitucional que han de ser tomados en consideración a la hora de emitir una orden de cesión de datos.

En cualquier caso, estos datos han de ser vistos desde la perspectiva de su dimensión estática; es decir, en tanto en cuanto representen, aparte de los simpes datos de conectividad, bien la sola aportación de información sobre quién está detrás realmente de una determinada identidad electrónica, o un hecho del pasado: una comunicación ya consumada o no llegada a buen fin, de cuya existencia dan fe precisamente concretos datos de tráfico. Y ello excluirá estos datos de la protección que ampara el secreto de las comunicaciones en base, en nuestro ordenamiento constitucional, al art. 18.3 de la Constitución Española -CE-[47].

---

[46] Por poner ejemplos, *TELEGRAM* conserva la información compartida en su sistema de almacenamiento, pero lo hace con herramientas de encriptación solamente accesibles a los concretos usuarios; *SIGNAL* optó en su día por realizar labores de tránsito e intermediación, no conservando más información que datos sobre los números de teléfono de sus usuarios.

[47] No abordaremos con el detenimiento que se merece la compleja cuestión sobre esa dimensión estática o dinámica del secreto de las comunicaciones en nuestro ordenamiento jurídico, sobre la que tanto ha hablado ya nuestra doctrina. Pese a que la jurisprudencia de nuestro Tribunal Constitucional sigue mostrándose de forma preocupantemente dubitativa (véase en este sentido la más reciente STC 99/2021, y su contraste con sus precedentes de las SSTC 114/1984, de 29 de noviembre; 70/2002, de 3 de abril; 123/2002, de 20 de mayo; 170/2013, de 7 de octubre, y 145/2014, de 22 de septiembre), la jurisprudencia de la Sala 2ª del Tribunal Supremo (por citar como ejemplos más recientes las ya referidas SSTS 824/2022, de 19 de octubre, y 199/2023, de 21 de marzo) se decanta de manera abrumadora por la exclusión de la protección formal del secreto una vez que la comunicación puede entenderse consumada. A nivel doctrinal, podemos citar como uno de los últimos ejemplos coincidentes con tal planteamiento a OCÓN GARCÍA, Juan (*"Derecho fundamental al secreto y tecnologías avanzadas de comunicación"*. Centro de Estudios Políticos y Constitucionales; Primera Edición. Madrid, 2021; pág. 36), así como los autores que cita. Pero el salto definitivo ha de encontrarse sin duda en la STEDH, Secc. 3ª, de 8 de noviembre de 2016 (caso FIGUEIREDO TEIXEIRA v. Andorra; asunto 72684/14); donde, analizándose precisamente un supuesto de una orden cesión de datos de tráfico dirigida a operadora de telecomunicaciones, en ningún momento la sentencia llega a residenciar el ámbito jurídico afectado en el contexto del derecho a la correspondencia, sino exclusivamente en el derecho a la vida privada de la persona afectada por la medida. En este sentido, y en relación al estudio del concepto y alcance del derecho al respeto de la correspondencia a que se refiere el art. 8.1 del CEDH, BREITENMOSER, Stephan (*"Der schutz del Privatsphäre Gemäs art. 8 EMRK";* Editores Helhing y Lichitenhahn. Basilea, 1986 Basilea, 1986), citado a su vez por MORENILLA RODRÍGUEZ, José María (*"El respeto a la esfera privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos"*; en La jurisprudencia del Tribunal Europeo de Derechos Humanos. Cuader-

La STJUE del caso LA QUADRATURE DU NET perfila con claridad lo que es la cesión de datos en cualquiera de sus formas, frente a lo que es una emisión de una orden de interceptación de datos de tráfico y de localización en tiempo real. Y lo hace en consonancia con un art. 5.1 de la Directiva 2002/58/CE que habla de garantía, no del respeto de las comunicaciones que a toda persona reconoce el art. 7 de la CDFUE, sino de la confidencialidad de las comunicaciones; como vínculo contractual que une al prestador de servicios de comunicaciones electrónicas con su cliente. Realmente, ese principio de confidencialidad abarcará tanto a contenidos como a datos de tráfico, en tanto que la comunicación se encuentra en tránsito pero también, y como datos personales, a esos mismos datos de tráfico, referidos a comunicaciones ya consumadas, en tanto que han de ser almacenados y tratados para alguna de las finalidades que previene el art. 6. Por eso, la norma establece la prohibición de *"…la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados…"*. Debe apreciarse, de hecho, cómo el legislador comunitario dedica el contenido esencial de la Directiva precisamente a ese momento en que el dato de tráfico pierde protagonismo, una vez que la comunicación ha llegado a buen fin o ha resultado finalmente frustrada. Solamente en cuanto respecta al vínculo funcional del dato de tráfico con el tránsito de una comunicación, el art. 6.1 muestra una preocupación por éste; aunque haciéndolo convivir con ese mismo dato que ha de permanecer conservado, una vez ultimada la comunicación, por otros motivos técnicos o a los efectos de lo previsto en el apartado siguiente del mismo precepto.

La posición del Convenio de Budapest en este sentido se nos antoja aún más taxativa. Al igual que planteara la mencionada sentencia del TJUE, el Convenio diferencia claramente la incautación de datos de tráfico o contenidos en el curso de un registro de dispositivo de almacenamiento masivo de datos, incluida su expansión a otros repositorios de datos a disposición de aquéllos o consecuencia de la emisión u órdenes de cesión de datos -art. 18 y 19.2-, de lo que serían órdenes de interceptación en tiempo real. Pero es que en interpretación de la primera de las dos normas, el Informe Explicativo al Convenio, en su §190 no describe otro posible punto de fricción en orden a la consideración o no del dato de tráfico, e incluso contenido, estático, que el supuesto en el que un mensaje de correo electrónico es encontrado sin haber sido leído o abierto; única hipótesis en que se muestra comprensivo de la existencia, en tales hipótesis, de ordenamientos nacionales reacios a desgajar el supuesto del manto protector del secreto de las comunicaciones[48].

---

nos de Derecho Judicial. CGPJ, Madrid 1993; pág. 293), concluía que la protección del derecho al respeto de la correspondencia, frente a injerencias externas, alcanzaría desde el envío hasta la recepción; de lo que deducía que quedarían fuera de este ámbito concreto de protección las cartas no enviadas o de comunicaciones no escritas, que lo serían bajo otras diversas dimensiones de ese tronco común de la privacidad tales como la protección del respeto de la vida privada o del domicilio.

[48] "*190. El Artículo 19 se aplica a los datos informáticos almacenados. Respecto de esto, se plantea la cuestión de si un mensaje de correo electrónico no abierto que se encuentra en el buzón de entrada de mensajes de un proveedor de Internet hasta que el destinatario lo descargue a su sistema informático, debe considerarse datos informáticos almacenados, o datos en proceso de transferencia. Conforme a las leyes de algunas Partes, ese mensaje de correo electrónico es parte de una comunicación y, por consiguiente, su contenido sólo puede obtenerse aplicando la facultad de interceptación; por el contrario, otros sistemas jurídicos consideran dicho mensaje como datos almacenados a los que corresponde aplicar el Artículo 19. Por consiguiente, las Partes deberían analizar su legislación respecto de esta cuestión*

Al menos desde la perspectiva transnacional, de los textos normativos que abordan la cuestión de la cesión de datos relativos a las comunicaciones, esta clara diferenciación que se establece en función de la caracterización de la orden de cesión como ejecutable en tiempo real frente a la cesión de datos conservados de comunicaciones pretéritas deja muy poco margen de discusión.

B) La cesión de datos de tráfico o localización conservados por motivos comerciales. en el curso de una investigación criminal en la jurisprudencia del TJUE

El primer abordaje directo que el Tribunal de Luxemburgo acometiera a la cesión de datos comerciales en el contexto de una investigación criminal sería consecuencia de un auténtico accidente. Cuando la Sección 3ª de la Audiencia Provincial de Tarragona decidió plantear la cuestión prejudicial que fuera tramitada por el TJUE con el número C-207/16 -STJUE (Gran Sala) de 2 de octubre de 2018 (caso MINISTERIO FISCAL, asunto C- 207/16)- partía de la consigna de confrontar la legislación española sobre conservación de datos con unos precedentes jurisprudenciales del TJUE manifiestamente contrarios a la conformidad de los regímenes de conservación preventiva e indiscriminada con el Derecho de la Unión. Pero partía de una premisa errónea: considerar que la información que guardan las operadoras de comunicaciones sobre la conjunción entre IMSI e IMEI de un dispositivo móvil de comunicaciones era un dato que podía obtenerse de conformidad con el mandato del art. 1 de la LCDCE. Muy al contrario, el TJUE es consciente del diverso origen de la fuente de información que se interesaba del Juzgado de Instrucción[49]; y de forma palmaria desoye el intento de pronunciamiento sobre la más que discutible conformidad de la ley española con dicha jurisprudencia, limitándose a valorar si la concreta cesión de datos, en un contexto de proporcionalidad de la medida, se ajustaba a los cánones permitidos por el art. 15.1 de la Directiva 2002/58/CE. Contestaba en este sentido a la cuestión prejudicial diciendo que dicho precepto: *"…a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, consagrados en los citados artículos de la Carta de los Derechos Fundamentales, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave".*

La STJUE del caso LA QUADRATURE DU NET y otros tampoco aportará una información clara sobre el posicionamiento del Alto Tribunal europeo; más allá de la lectura que puede inferirse a cuestiones genéricas que atañen a una cierta evolución en cuanto a la debida ponderación del principio de proporcionalidad; a las exigencias propias de la necesaria puesta en conocimiento a los interesados afectados del acto de injerencia, y, mediante el acercamiento al supuesto de tratamiento automatizado de datos de tráfico y localización en el contexto de una investigación criminal o injerencias en tiempo real, a su relación con las exigencias propias del Reglamento (UE) 2016/679.

---

para determinar lo que es apropiado con arreglo a sus respectivos ordenamientos jurídicos" (fuente: ETS 185 Explanatory report_Spanish (coe.int)).

[49] Se trataba de identificar la tarjeta SIM asociada a un teléfono móvil objeto de un robo en el que se empleara una inusitada violencia, como forma de tratar de identificar a los autores del robo.

Para comprender cuál es la posición del TJUE sobre la cesión de datos conservados por las operadoras por motivos comerciales habríamos de esperar a la más reciente STJUE (Sala Sexta) de 17 de noviembre de 2022 (caso SPETSIALIZIRAN NAKAZATELEN SAD; asunto C-350/21). La cuestión prejudicial volvía a jugar, como sucediera con el precedente del caso MINISTERIO FISCAL, con conceptos relacionados con la conservación preventiva e indiscriminada de datos. Sin embargo, nos encontramos con pronunciamientos que, respondiendo a la cuestión, son predicables perfectamente de las órdenes de cesión de datos, como sucede con la indiscutible aplicación del principio de necesidad a medidas conservación/cesión de datos[50]; y que, ya específicamente genuinos de lo que sería cesión de datos conservados por motivos comerciales, atañen al reconocimiento del derecho de información de las personas concernidas y establecimiento de recursos y remedios procesales efectivos contra las órdenes de cesión[51]. A partir de aquí, solamente restará encontrar referentes sobre la cualidad de la autoridad de decisión y control, especialmente en las sentencias de los casos TELE2 SVERIGE AB y otros y PROKURATUR así como una mención genérica al deber de motivación y su relación con las posibilidades de control externo de la decisión en la más reciente STJUE (Sala Tercera) de 16 de febrero de 2023 (asunto C-349/21).

Interesa sobre todo el genuino tratamiento que dispensa el TJUE al principio de proporcionalidad en el que partirá de un esquema que nos previene de la imposibilidad de establecer espacios de exclusión del principio de protección de la confidencialidad de las comunicaciones y los datos de tráfico y localización con ella relacionados. Así nos lo dirá el §51 de la sentencia del caso MINISTERIO FISCAL, al advertirnos de que, por muy liviana que fuera la injerencia, seguiríamos enfrentándonos, como consecuencia de una orden de cesión de datos, a la necesidad de superar el juicio de proporcionalidad que impone el art. 15.1 de la Directiva 2002/58/CE; que, *«...incluso a falta de circunstancias que permitan calificar esta injerencia de "grave" y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia».* Pero también nos enfrentará a la otra cara de la moneda; al indicarnos que el concepto de lucha contra la delincuencia que maneja el mencionado precepto no es exclusivo en modo alguno de la lucha contra la delincuencia grave -§54-[52].

Es a partir de este momento donde la capacidad innovativa del TJUE alcanza su cénit. El término de comparación en el juicio ponderativo entre el interés del ciudadano en verse preservado en su derecho a la privacidad y el fin público de persecución del delito y del delincuente se definirá en consonancia con los más graves niveles de afectación de tal interés. Ese nivel máximo de injerencia se correspondería con lo que describe como aquellos datos perso-

---

[50] *" L'article 15, paragraphe 1, de la directive 2002/58/CE...[...]...doivent être interprété en ce sens qu'il s'oppose :...*
– à une législation nationale ne prévoyant pas, de manière claire et précise, que l'accès aux données conservées est limité à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi par cette conservation".

[51] *"L'article 15, paragraphe 1, de la directive 2002/58...[...]...doivent être interprétés en ce sens que : ils s'opposent à une législation nationale prévoyant l'accès, par les autorités nationales compétentes en matière d'enquêtes pénales, à des données relatives au trafic et à des données de localisation, conservées de manière licite, sans garantir que les personnes dont les données ont fait l'objet d'un accès par ces autorités nationales en soient informées dans la mesure prévue par le droit de l'Union, et sans qu'elles disposent d'une voie de recours à l'encontre d'un accès illégal à ces données".*

[52] *"...*(E)*l tenor del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general"*

nales conservados por los proveedores que, "*...considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados".*

El otro lado de la balanza vendrá relacionado con el concepto de *delincuencia grave.* Solamente la lucha contra la delincuencia grave podría justificar una injerencia que alcanzara tal nivel de afectación capaz de generar perfiles detallados sobre la vida de las personas sometidas a investigación. La sentencia comentada, acudiendo a lo que se nos dijera, con carácter ejemplificativo, en el Preámbulo de la Directiva 2006/24/CE, al que igualmente acudiera la STJUE del caso TELE2 SVERIGE AB y otros, opta por hacer una mención expresa a lo que se define como delincuencia organizada y terrorismo. Ello no significará en modo alguno que no existan otros bienes jurídicos o finalidades legítimas que permitieran alcanzar ese máximo nivel de injerencia[53].

Ese carácter ejemplificativo habría de conectarse indiscutiblemente con la posibilidad de dar protección a otros valores jurídicos de especial trascendencia. Así, y aparte de determinadas normas del Derecho de la Unión exigentes de elevados niveles de protección[54], se manifestaría en primer lugar la STJUE del caso LA QUADRATURE DU NET y otros. Frente a la hábil cita por la *Cour Constitutionnelle* belga de la STEDH, Sección 4ª, de 2 de diciembre de 2008 (caso K.U. v. Finlandia; asunto 2872/02), el TJUE se ve en la necesidad de abrir el concepto hacia la protección de determinados bienes jurídicos prevalentes, entre los que se encontraría sin duda, la lucha frente a los abusos sexuales contra menores en red; y más en concreto, *"...cuando existe una amenaza para el bienestar físico y moral de un niño"*; lo que habría de comportar sin duda la necesidad de habilitar las normas sustantivas y procesales adecuadas para la salvaguardia de ese bien superior, dentro de los oportunos márgenes de proporcionalidad, mediante el diseño de un *"...marco jurídico que permita conciliar los distintos intereses y derechos que se han de proteger".* La siguiente sentencia del caso G.D. y COMISSIONER AN GARDA SÍOCHÁNA recoge la antorcha de este planteamiento, expandiendo estos supuestos de valores jurídicos capaces de abrir las puertas a severas medidas injerenciales a otros en los que no se oculta un claro paralelismo con la jurisprudencia del TEDH[55]. Hablamos de determinados derechos fundamentales garantidos por la CDFUE, tales como el derecho a la integridad personal –art. 3-, la prohibición de la tortura y tratos inhuma-

---

[53] En este sentido En este sentido, RODRÍGUEZ LAINZ, José Luis., *"La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada…"*; op. cit.

[54] RODRÍGUEZ LAINZ (op. cit.) pondría los ejemplos de la Directiva 2011/36/UE del Parlamento Europeo y del Consejo de 5 abril de 2011, relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas y por la que se sustituye la Decisión marco 2002/629/JAI del Consejo y la Directiva 2011/92/UE, del Parlamento Europeo y del Consejo de 13 de diciembre, relativa a la lucha contra los abusos sexuales y la pornografía infantil y por la que se sustituye la Decisión Marco 2004/68/JAI del Consejo. Debe recordarse, igualmente cómo la STJUE (Gran Sala) de 20 de septiembre de 2022 (casos VD y SR; asuntos C-339 y 397/20), abre las puertas a injerencias de tal naturaleza en materia de amenazas contra ataques a la integridad de los mercados financieros de la Unión Europea y la confianza del público en los instrumentos financieros (Directiva 2003/6/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, sobre las operaciones con información privilegiada y la manipulación del mercado (abuso del mercado), en relación con el Reglamento (UE) n.º 2014/596 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado (Reglamento sobre abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión).

[55] RÓDRÍGUEZ LAINZ (ídem).

nos o degradantes -art. 4-, la libertad y seguridad –art. 6- y, en términos generales, la privacidad –art. 7-[56]. Ahora bien, de la lectura del mismo §50 se infiere con claridad cómo no basta con la salvaguardia de estos nuevos derechos para poder acceder a las más severas representaciones de la excepción al mandato protector del art. 15.1 de la Directiva 2002/58/CE. Se impone un segundo nivel de proporcionalidad que habrá de mitigar, en el caso concreto, el rigor de ese criterio ponderativo. La defensa de estos nuevos valores podría justificar sin duda la emisión de órdenes de cesión de datos relativos a comunicaciones de personas investigadas; pero para alcanzar a esas cotas que abrieran las puertas a aquellos datos que, en su conjunto, permitieran extraer datos precisos sobre la vida de las personas cuyos datos han sido conservados, debería confrontarse un interés público especialmente intenso, caracterizado por una muy grave afectación de tales valores. Para identificar al autor de una agresión, afectante al derecho a la integridad física de la persona lesionada, no podría acudirse a la cesión de todos los datos de localización de personas bajo el radio de acción de una estación BTS en una determinada franja temporal; pero si la agresión produce severas lesiones, y el delito se comete por grupo con una marcada intencionalidad de discriminación por orientación sexual o por razón de la raza de la víctima, ese planteamiento podría variar según las circunstancias.

El criterio penológico, tan afincado en nuestro entorno sustantivo y procesal más cercano, no encontró, sin embargo, una acogida explícita en la jurisprudencia del TJUE comentada. Podríamos encontrar una referencia implícita al criterio de la mayor severidad en el reproche punitivo como definidor del concepto de delito grave en alguna norma del acervo comunitario como ocurriera con el art. 15.3 de la Directiva 2011/92/CE, al establecer como uno de los criterios moduladores de la intensidad de la injerencia a los efectos de definir la concreta medida tecnológica, *"…la índole y gravedad de las infracciones que se estén investigando"*. Pero el Tribunal de Luxemburgo obra con cautela en este punto; plenamente conocedor de las grandes disparidades existentes en la determinación de penas por unos mismos hechos en los ordenamientos jurídicos de los Estados miembros, así como en la extensión del arco penológico[57]. Aventurar en este sentido un pronunciamiento sobre si una pena de hasta

---

[56] *"Ahora bien, en la medida en que permite a los Estados miembros limitar los derechos y las obligaciones mencionados en los apartados 34 a 37 de la presente sentencia, el artículo 15, apartado 1, de la Directiva 2002/58 refleja el hecho de que los derechos consagrados en los artículos 7, 8 y 11 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse de acuerdo con su función en la sociedad. En efecto, como se desprende del artículo 52, apartado 1, de la Carta, esta admite limitaciones al ejercicio de esos derechos, siempre que se establezcan por ley, respeten el contenido esencial de los citados derechos y, ajustándose al principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás. De este modo, la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 a la luz de la Carta exige tener en cuenta asimismo la importancia de los derechos consagrados en los artículos 3, 4, 6 y 7 de la Carta y la que presentan los objetivos de protección de la seguridad nacional y de lucha contra la delincuencia grave al contribuir a la protección de los derechos y de las libertades de terceros (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 120 a 122 y jurisprudencia citada)"* -§ 50-.

[57] En el background del contexto en que se gestara la sentencia del caso MINISTERIO FISCAL, BAHAMONDE BLANCO, Miriam (*"Medidas de investigación tecnológica a la luz de los Derechos Fundamentales, una cuestión pendiente"* (Diario La Ley, Nº 9160, Sección Tribuna, 16 de Marzo de 2018, Editorial Wolters Kluwer)), hacía especial mención al alegato defendido por el representante de Dinamarca; quien sacaba a relucir cómo *"... en su país las penas se definen de forma más leve que en otros Estados pues no se concibe la dureza punitiva como el mecanismo para terminar con la delincuencia (así, un deli-*

cinco años de prisión debiera considerarse grave, a los efectos de la reputación del hecho como delito grave, era, sin duda, arriesgado. Por eso, tal vez pudiéramos entender que, aunque dicho criterio puede aportar un indicio determinante de la gravedad de determinada infracción criminal, su trascendencia indiscutible habría de reservarse a los efectos del sometimiento de la decisión de la autoridad competente al segundo juicio de proporcionalidad de su aplicación en el caso concreto.

Hasta ahora hemos definido ese nivel máximo de injerencia que se relaciona con el riesgo de generación de perfiles detallados sobre rasgos de personalidad de las personas sometidas a vigilancia. Sin embargo, ello no significa en modo alguno que la jurisprudencia del TJUE se cierre en banda a cualquier aplicación de medidas de investigación basadas en el aporte de información sobre datos relativos a las comunicaciones en general, o datos de tráfico o de localización en concreto. La sentencia del caso MINISTERIO FISCAL introduce, de hecho, un criterio escalar decreciente; en virtud del cual, a menor intensidad en la injerencia, menor exigencia en la gravedad de la infracción criminal objeto de investigación que le sirviera de fundamento. La lectura conjunta de sus de sus §§56 y 57 no podría dejar duda alguna al respecto; pues, si en base a la vigencia del principio de proporcionalidad en el ámbito de la investigación criminal, solo sería justificable aquella injerencia grave cuyo objetivo fuera *"…luchar contra la delincuencia que a su vez esté también calificada de «grave»"*; continuará aclarando que, *"…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"*.

En el caso concreto del caso MINISTERIO FISCAL, el TJUE consideró que un acceso a información sobre relación entre concreto IMEI de un teléfono sustraído e IMSI que pudieran haberse introducido en el terminal físico durante una breve franja de tiempo (12 días), y su relación con concretas titularidades de las tarjetas SIM detectadas no comportaba en modo alguno una injerencia grave por lo que el acto de injerencia por el que se planteara la cuestión prejudicial sería perfectamente predicable de un delito de robo con violencia como el que era objeto de investigación. Ello, nos dirá *"…no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave"* -§63-[58].

Esta escala decreciente sería la que, a la postre, permitirá expandir en la sentencia del caso LA QUADRATURE DU NET y otros el ámbito de aplicación de la excepción contenida en el art. 15.1 de la Directiva 2002/58/CE a regímenes de conservación preventiva e indiscriminada de datos a los datos de identidad civil. Pero el parágrafo 71 de la STJUE del caso G.D. y COMISSIONER AN GARDA SÍOCHÁNA parece contradecirse con la clara alineación que precede con el criterio mantenido comúnmente con la sentencia del caso MINISTERIO FISCAL en su §56; toda vez que, al menos de forma explícita, se relaciona la posible utilización de datos de identidad civil procedentes de bases de datos impuestas por la ley nacional con carácter preventivo e indiscriminado también con la lucha contra la delincuencia grave[59]. La propia sentencia define los datos de identidad civil como aquellos datos precisos

to de pornografía infantil, que en Dinamarca es delito grave, está sancionado con pena de un año de prisión)".

[58] En el mismo sentido se pronuncia el § 59 de la STJUE del caso LA QUADRATURE DU NET y otros.

[59] *"A este respecto, consta que la conservación de los datos relativos a la identidad civil de los usuarios de los medios de comunicación electrónica puede contribuir a la lucha contra la delincuencia grave,*

que *"...permitan identificar a las personas que han utilizado tales medios en el contexto de la preparación o la comisión de un acto delictivo grave"*. Solo cruzando éstos con los contenidos de datos de tráfico o de localización de concretas comunicaciones, podrían adquirir una especial relevancia pero por su relación con éstos y en base a un conocimiento de los mismos que debe suponerse legítimo. Representan por ello el más genuino ejemplo de mínima intensidad en la injerencia que abriría las puertas para su utilización *para perseguir delitos en general*. Quizá deba de darse sentido a este evidente alejamiento de la posición anterior, aparte de supuestos en los que se haya realizado un análisis masivo de datos identitarios, en el origen mismo de la fuente: una base de datos impuesta con carácter preventivo para facilitar ulteriores investigaciones criminales; lo cual contrastaría con unos datos de identidad civil, conservados por motivos comerciales por las operadoras de telecomunicaciones de forma lícita, cuando menos durante la duración de la relación contractual. Nada habría de impedir, al menos en mi opinión, y siempre con una adecuada ponderación de los principios de proporcionalidad y necesidad, expandir la posibilidad de acceso a concretos datos identitarios, cuando éstos tienen su origen en datos conservados por las operadoras por motivos comerciales.

La sentencia del caso SPETSIALIZIRAN NAKAZATELEN SAD centrará su análisis en la posibilidad de cesión de datos de tráfico y localización conservados por las operadoras por motivos comerciales, en aplicación de los arts. 5, 6 o 9 de la Directiva 2002/58/CE -§62-. Y éstos sí son sometidos, por su especial trascendencia y potencialidad de poderse derivar de su análisis conjunto la obtención de esas conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservado que tanto preocupa al Alto Tribunal, a una exigencia de limitación tan solo para la lucha contra la delincuencia grave.

Precisamente en el campo de las posibilidades de cesión de datos por decisión de una autoridad competente, esta sentencia intensifica su apuesta por la implicación del segundo gran principio rector: el principio de necesidad de la medida. La sentencia, que considera en su §63 al principio de necesidad como un componente más del principio de proporcionalidad en sentido amplio, impone una estricta sujeción a un tal principio; que es entendido como la exigencia de que la normativa nacional imponga, de forma clara y precisa, que el acceso a tales datos lo sea dentro de lo estrictamente necesario para obtener tal objetivo, y siempre dentro de los márgenes exigidos por las normas sobre protección de datos personales. La sentencia trae a colación el precedente de la sentencia del caso PROKURATUR, para recordarnos que la norma nacional habilitante debe garantizar *"...que tanto la categoría o categorías de datos mencionados como el período durante el cual se solicita el acceso a ellos se limiten, en función de las circunstancias del caso, a lo estrictamente necesario para los fines de la investigación de que se trate"*[60].

---

siempre que esos datos permitan identificar a las personas que han utilizado tales medios en el contexto de la preparación o la comisión de un acto delictivo grave".

[60] *"S'agissant du point de savoir si la législation nationale concernée doit prévoir, de manière claire et précise, que l'accès aux données conservées est limité à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi par cette conservation, il ressort de la jurisprudence que, pour satisfaire à l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, il appartient aux autorités nationales compétentes d'assurer, dans chaque cas d'espèce, que tant la ou les catégories de données visées que la durée pour laquelle l'accès à celles-ci est sollicité soient, en fonction des circonstances de l'espèce, limitées à ce qui est strictement nécessaire aux fins de l'enquête en cause [arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 38 et jurisprudence citée]".*

Esta exigencia de previsión de las debidas garantías en orden a la salvaguardia del principio de necesidad, y, por ende, del principio de proporcionalidad, se traduce en un enfatizado deber de calidad en la norma nacional habilitante de suerte que esta norma habrá de establecer normas claras y precisas que regulen el alcance y aplicación de la medida controvertida, e imponga requisitos mínimos dirigidos a garantizar que la aplicación de la norma solo permitirá el acceso a los datos conservados en cuanto que sea estrictamente necesario para alcanzar el objetivo perseguido. Para ello habrá de atender a dos finalidades muy concretas, claramente asociadas con las exigencias de la doctrina del TEDH en relación con la exigencia de la calidad de la norma habilitante: Por una parte, la cognoscibilidad por cualquier ciudadano de cómo y bajo qué circunstancias habrían de verse afectados por una tal medida de injerencia, y, sobre todo que dichas normas puedan protegerles de manera efectiva contra los riesgos de abuso o arbitrariedad -§§64, 65 y 67-.

Tales exigencias tendrán una íntima relación con el deber que han de asumir los Estados miembros no solo de establecer una perfecta perfilación de esa estricta finalidad que abrirá las puertas a la emisión de una orden de cesión de datos, sino, también, y muy especialmente, a las condiciones materiales y procedimentales que regulen dicha utilización. Finalidad, presupuestos legales de aplicación y procedimiento adquieren por ello un indiscutible protagonismo en esta exigencia de calidad de la norma habilitante. Y la conjunción de procedimiento y garantías para los ciudadanos afectados ha de traducirse, sin duda, en la definición de efectivas herramientas reaccionales en su favor.

Es aquí cuando la sentencia del caso SPETSIALIZIRAN NAKAZATELEN SAD enlaza con el mandato normativo de la Directiva (UE) 2016/680; como referente incontestable para servir de fundamento a cualesquiera órdenes de cesión de datos relativos a las comunicaciones conservados por las operadoras por motivos comerciales, tal y como se infiere de sus art. 2.1 y 8. Pero lo hace no tanto para buscar un fundamento para justificar la licitud de este tipo de órdenes de cesión de datos dirigidas a la lucha contra la delincuencia, que ya encontrarían precisamente su fundamento en el mandato del art. 15.1 de la Directiva 2002/58/CE, como para hacer especial hincapié en ese derecho de información que adquiere tanto protagonismo en la norma con sus arts. 12 y 13 y del que se derivarán, aunque no se diga expresamente en la sentencia, otros derechos del orden de la protección de datos personales (acceso, rectificación, supresión y limitación). Se garantizará por la referida sentencia, con apoyo en el precedente de la STJUE de 21 de diciembre de 2016 (caso TELE2 SVERIGE y WATSON y otros), esta exigencia de tal deber de comunicación individualizado, en el marco de los procedimientos nacionales aplicables pero en el buen entendimiento de que ello no pueda poner en peligro las investigaciones efectuadas por dichas autoridades -§70-[61]. Concluirá, por ello, advirtiendo que, *"…si bien los Estados miembros pueden adoptar medidas legislativas para retrasar, limitar o incluso eliminar el suministro de información al interesado, siempre que tal medida cumpla los requisitos establecidos en el apartado 3 de este artículo, una legislación nacional que excluya, en general, todo derecho a la información no es conforme con el Derecho de la UE"*[62].

[61] En el mismo sentido, el referente a los arts. 16.4 y 18 de la Directiva (UE) 2016/680.

[62] *"Or, cette obligation d'information de la personne concernée a été confirmée à l'article 13 de la directive 2016/680, dont il ressort que, si les États membres peuvent adopter des mesures législatives visant à retarder, à limiter ou même à supprimer la fourniture des informations à la personne concernée, pour autant qu'une telle mesure soit conforme aux exigences énoncées au paragraphe 3 de cet article, une ré-*

La garantía de acceso a recursos efectivos se traduce en referencia a esa misma garantía que se reconocerá en los arts. 15.2 de la Directiva 2002/58/CE y 79 del Reglamento (UE) 2016/679. El propio Tribunal reconoce que, a falta de norma comunitaria, corresponde a los Estados miembros regular en su Derecho interno el adecuado régimen de recursos en favor de los justiciables, como consecuencia de una vulneración de los derechos que tienen garantidos por estas normas de protección de datos personales. Pero nos recordará que dichos regímenes han de respetar los principios de equivalencia y efectividad del Derecho de la Unión.

Descendiendo al nivel de la resolución habilitante, la jurisprudencia del TJUE es consciente de que de poco sirve una legislación estricta que imponga rigorosos niveles de garantía en la salvaguardia de los derechos fundamentales afectados y evitación de riesgos de abuso o arbitrariedad en su aplicación, si no va acompañada de una práctica forense que asuma el cometido de adaptar la norma al caso concreto pero haciéndolo, además, con un mínimo nivel de motivación, justificación, que cumpla con esa exigencia de cognoscibilidad que permita a los órganos de control realizar una valoración externa, y a las partes afectadas tomar conocimiento de las razones que están detrás de la decisión para poder obrar en consecuencia en el desarrollo de sus estrategias procesales. La polémica STJUE (Sala Tercera) de 16 de febrero de 2023 (asunto C-349/21) asumió el comprometido reto de determinar si modelos impresos de autorización de injerencias sobre comunicaciones, y sin más contenido motivador que el de una genérica referencia a que la solicitud policial o fiscal cumplía las exigencias de una legislación como la búlgara en materia de interceptación de comunicaciones, cumplía con ese nivel de fundamentación que habría de estar detrás de toda resolución habilitante basada en el art. 15.1 de la Directiva 2002/58/CE, en orden a exteriorizar los juicios de inferencia en cuanto a los hechos y la superación de los distintos juicios de valor que están detrás de los primordiales principios de proporcionalidad y necesidad.

La respuesta que nos dio el TJUE fue sin duda decepcionante: Una motivación por remisión como la indicada superaría las exigencias mínimas de cognoscibilidad del contenido motivador derivado del respeto del derecho a un juicio equitativo al que se refiere el art. 47.3 de la CDFUE, con tal que una *lectura cruzada* de solicitud y autorización permitiera, *de una forma fácil y sin ambigüedad*, tomar conocimiento de las razones por las cuales se autorizó la medida. Y ello, independientemente de que la resolución sea en si misma un documento abstracto que, con plena delegación al contenido motivador de la solicitud, no permitiera realizar un juicio externo. Pero no nos interesa tanto someter a una severa crítica tal planteamiento[63], tan alejado de los estándares impuestos a nivel de nuestra legislación interna, como analizar el fundamento y alcance de esta doctrina.

La exigencia de motivación encuentra encaje en la jurisprudencia del TJUE en una doble vertiente: Por un lado, por ser una exigencia de cualquier resolución que suponga la res-

glementation nationale qui exclurait, de manière générale, tout droit à l'information ne serait pas conforme au droit de l'Union".

[63] La sola confrontación con la STEDH Secc. 4ª, de 11 de enero de 2022 (caso EKIMDZHIEV y otros v. Bulgaria; asunto 70078/12), que incluso se atreve a citar el TJUE, muestra cómo de forzado es el discurso jurídico de la STJUE de 16 de febrero de 2023. El § 63 de esta sentencia sale al paso del difícil reto de conciliar su doctrina con una posición del TEDH que ve no tanto en la ley, como en la viciada aplicación cotidiana de la misma por los tribunales húngaros, una prueba de la insuficiencia de la ley para cumplir con los objetivos derivados del principio de la calidad de la norma habilitante, basándose en abrumadores criterios estadísticos. Hablar por ello del respeto del principio de equiparación derivado del art. 52.3 de la CDFUE se nos antoja, cuando menos, discutible.

tricción de derechos fundamentales, y de la que no se escaparían, lógicamente, las excepciones individualizadas a la norma prohibitiva del tan citado art. 15.1 de la Directiva 2002/24/CE; por otro, esa garantía del derecho a un juicio equitativo, que impone a las autoridades competentes exteriorizar las razones por las cuales se ha adoptado una determinada decisión, permitiendo a éstas, en base a ellos, desplegar sus estrategias reaccionales.

A la hora de analizar ese primer pilar del deber de motivación, la STJUE de 16 de febrero de 2023 acudió al precedente de la STJUE del caso PROKURATUR; del que extraía la necesidad de ponderación de los requisitos materiales y formales que son impuestos por la norma nacional. Efectivamente, difícil sería comprender que la exigencia se limitara al examen de la previsión normativa sobre tales requisitos materiales y formales mas no al deber de ponderación del cumplimiento de unas y otras -§42-. Sin esta ponderación, la respetuosa previsión de la norma quedaría huera de sentido[64].

El siguiente pilar enraíza profundamente con el anterior. Si el deber de motivación asume el cometido de exteriorizar las razones por las que la autoridad competente adopta la medida restrictiva, estará asumiendo a su vez un marcado carácter instrumental y finalístico dirigido a dar cumplimiento a la exigencia del derecho a un proceso equitativo. Por tal razón, la sentencia, en su §44, concebirá la exigencia de motivación como uno de los componentes fundamentales de la garantía que representa el derecho al juicio equitativo. Estamos penetrando, con ello, en el ámbito propio y genuino del deber de motivación; que el derecho a un proceso equitativo reconocido en el 47.2 de la CDFUE, *"…requiere que toda resolución judicial se motive"*.

Este juicio externo que deberá facilitarse a las partes interesadas a través de la motivación, nos diría el §59, debería poderse realizar de modo que la resolución habilitante permitiera a las partes interesadas, y obviamente a autoridades de control, de una forma fácil y sin ambigüedad, una comprensión de las razones que están detrás de la decisión pudiendo llevarse a efecto *"…mediante una lectura cruzada de la autorización para usar técnicas especiales de investigación y de la solicitud motivada que la acompaña"*. El contenido mínimo de la motivación deberá abarcar, nos dirá, tanto a "…*las razones precisas por las que se concedió a la vista de los elementos fácticos y jurídicos que caracterizan el caso individual al que se refiere la solicitud"*, como a la determinación del *"…período de validez de dicha autorización"*[65].

La determinación de la cualidad de la autoridad que puede adoptar una medida de excepción a la norma prohibitiva del art. 15.1 de la Directiva 2002/58/CE es objeto de especial preocupación para el TJUE. Si ya la STJUE de 21 de diciembre de 2016 mostrara su oposición a la consideración del Ministerio Fiscal como posible autoridad decisora para ordenar una cesión de datos conservados, la sentencia del caso PROKURATUR parece decantarse por la idea de privar al Ministerio Público de capacidad de decisión propia en cuanto al acceso, en

[64] La STJUE del caso PROKURATUR, de hecho hizo, especial hincapié en exigir que el juicio de ponderación del juicio de proporcionalidad tuviera en cuenta la potencialidad invasiva de la resolución en función de la información que probablemente pudiera obtenerse como consecuencia de la aplicación de la medida de investigación; concluyendo en su parágrafo 40 que: *"…la apreciación de la gravedad de la injerencia del acceso se efectúa necesariamente en función del riesgo para la vida privada de las personas afectadas que suele corresponder a la categoría de datos solicitados, sin que, por otra parte, sea preciso saber si la información relativa a la vida privada que de ellos deriva es, en concreto, sensible o no"*.

[65] La sentencia analiza un supuesto de interceptación de comunicaciones en tiempo real en el que, obviamente, el factor tiempo, como determinante de los juicios de proporcionalidad, necesidad e idoneidad de la medida, adquiere una especial relevancia.

el contexto de una investigación criminal, a información sobre datos de tráfico o de localización[66]; y ello en base a ese doble cometido de dirección de la fase de investigación y parte acusadora. Por la misma razón, la STJUE del caso G.D. y COMISSIONER AN GARDA SÍOCHÁNA negaría tal cualidad a una autoridad policial, aunque se tratara de un superior jerárquico no directamente involucrado en la investigación. Podrá, eso sí, una autoridad judicial o autoridad administrativa independiente[67] tomar la decisión a petición de autoridad fiscal o policial.

Pero ello no significa que no puedan adoptarse determinadas medidas por autoridades administrativas o incluso fiscales, al menos en supuestos de actuación urgente. Esta última sentencia nos dejará bien claro que la intervención de la autoridad judicial o administrativa independiente no es la de fiscalizar a posteriori, vía recurso o posterior acto de supervisión; sino que se someta a ella la decisión misma, bien con carácter previo, bien mediante su ratificación para supuestos de urgencia -§110-.

Surge, sin embargo, la duda sobre cuál sería la postura del TJUE en relación con las órdenes de cesión de datos identitarios, en los que la ínfima intensidad de la injerencia parecería ajustarse mejor a esa posición de supervisión o control mediante daciones de cuenta o resolución de recursos que caracteriza a los ordenamientos nacionales de la Unión, y, en concreto, a España. La STEDH, Secc. 5ª, de 30 de enero de 2020 (caso BREYER v. Alemania; asunto 50001/12)[68] no llegó a plantear realmente objeción alguna al hecho de que, entre otras autoridades que tienen asumida la investigación de infracciones criminales, una autoridad fiscal, como la referida en el art. 112 de la Ley alemana de Telecomunicaciones -*Telekommunikationsgesetz*- pudiera ordenar una cesión de datos registrados con motivo de la adquisición y activación de una tarjeta de prepago de telefonía móvil.

Esa indiscutible menor potencialidad lesiva que puede deducirse de un manejo ponderado de dicha información podría abrir las puertas, sin duda, a una apertura del Alto Tribunal hacia la posibilidad de que fuera una autoridad fiscal o policial quien legítimamente pudiera emitir la orden de cesión de datos con tal que, en contrapartida, se reforzaran los mecanismos de fiscalización por parte de la autoridad judicial o administrativa independiente de referencia.

Para terminar con este apartado, la sentencia aborda la cuestión de la fuente ilícita, como consecuencia de cuestiones que se plantean en relación con órdenes de cesión de datos dictadas por autoridades nacionales en base a normas internas que han de considerarse contrarias al Derecho de la Unión. Pero lo hace no en un contexto de ponderar el régimen adecuado

---

[66] *"El artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales, debe interpretarse en el sentido de que se opone a una normativa nacional que atribuye competencia al Ministerio Fiscal —cuya función es dirigir el procedimiento de instrucción penal y ejercer, en su caso, la acusación pública en un procedimiento posterior— para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización a efectos de la instrucción penal".*

[67] La propia sentencia desarrolla los contornos y exigencias de independencia de esta figura en sus §§ 52 y ss. Sobre el particular, véase el trabajo de RODRÍGUEZ LAINZ, José Luis: "*La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación…"*; op. cit.

[68] Un primer estudio crítico a esta sentencia, en el contexto de su relación con el art. 15.1 de la directiva 2002/58/CE puede encontrarse en el trabajo de BERMEULEN, Judith (*"Bulk retention of private-sector subscriber data for governmental purposes does not violate the Convention: Breyer v. Germany"*; Fuente: https://strasbourgobservers.com/ 2020/03/05/ bulk-retention-of -private-sector-subscriber-data-for-govern mental-purposes-does-not-violate-the-convention-breyer-v-germany/).

de la valoración de la prueba ilícita desde la óptica del derecho a un proceso equitativo, sino de garantía del respeto de los principios de primacía, equivalencia y efectividad, en cuanto respecta a la aplicación e implementación de las normas comunitarias por parte de los Estados miembros. La jurisprudencia citada a partir de la sentencia del caso LA QUADRATURE DU NET y otros, si bien se muestra comprensiva con los más estrictos sistemas basados en la llamada *regla de exclusión* e irradiación de la nulidad de la fuente ilícita a las derivadas, llega a ajustarse a la más reciente doctrina del TEDH sobre el llamado *principio adversarial*. Este principio supone garantizar a los justiciables una posibilidad real de acceder, controlar y contradecir la eficacia, autenticidad y oportunidad de la obtención de la evidencia lastrada de un vicio de afectación de concretos derechos fundamentales. Debería por ello el juez nacional, nos dirán las dos sentencias comentadas, como predicado del principio de efectividad, descartar *"…la información y las pruebas que se han obtenido a través de una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión o incluso mediante el acceso de la autoridad competente a esos datos infringiendo dicho Derecho, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia, cuando estas personas no estén en condiciones de comentar eficazmente tal información y tales pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y que pueden influir destacadamente en la apreciación de los hechos".*

C) Sobre la conformidad del ordenamiento procesal penal español con las exigencias de la jurisprudencia del TJUE en materia de cesión de datos relativos a las comunicaciones conservados por motivos comerciales

El 588 ter j, indiscutible heredero del art. 310 del Borrador de Anteproyecto de Código Procesal Penal de 2012, asume el cometido de dar cobertura a las órdenes de cesión de datos obviamente relativos a comunicaciones electrónicas[69], y, además, en tanto que "…*se encuentren vinculados* [como sujetos obligados] *a procesos de comunicación"* -art. 588 ter j.1-. La norma identifica con aparente claridad a quienes participan en el proceso comunicativo en su condición de *prestadores de servicios*. Es este un concepto amplio que abarcaría sin duda, cuando menos, a los sujetos obligados referidos en la Directiva 2002/24/CE superando claramente al concepto de sujetos obligados a que se refiere el art. 2 de la LCDCE (*operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones*, en los términos referidos en la vigente LGT). De hecho, la norma, en su título, habla de *prestadores servicios*; y entre ellos distinguirá a los sometidos al mandato de la LCDCE y aquellos que los conserven *"…por propia iniciativa por motivos comerciales o de otra índole".* Además, la referencia que se hace al inicio del apartado 1 del precepto a *personas que faciliten la comunicación*, como confrontadas a los *prestadores de servicios*, abre las puertas, de la misma forma que hiciera el art. 588 ter e.1 de la LECRIM respecto de la interceptación de comunicaciones en tiempo real, a particulares que de alguna manera pudieran participar en la articulación de medios para facilitar el buen fin de una concreta comunicación. El supuesto del llamado *man in the middle* en la transmisión de comunicaciones a través de las conocidas como Redes TOR[70], y que actúan como nodos intermedios

[69] La sección en la que se introduce el precepto se define precisamente como: *Incorporación al proceso de datos electrónicos de tráfico o asociados.*

[70] En una red TOR los nodos intermedios actúan en una capa intermedia en la que de forma más o menos aleatoria el mensaje no se remite directamente al destinatario, sino que pasa por uno de estos nodos, sin

para impedir la trazabilidad de una comunicación transmitida a través de dichas redes, podría ser considerado como un ejemplo paradigmático de esta participación de particulares en concretos procesos comunicativos.

La fuente de información se somete igualmente a una generosa apertura: Datos conservados en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones -la LCDCE-, así como aquellos conservados por los sujetos obligados *por motivos comerciales o de otra índole*, siempre que respondan al denominador común de estar *vinculados a procesos de comunicación*. La participación del dato en un determinado proceso o procesos comunicativos, aunque fuere a nivel de conectividad, es la clave que permite la aplicación del comentado precepto. Los datos de identidad civil a que se refiere el art. 588 ter m habrían de ser recabados de los *"...prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o servicios de la sociedad de la información"* que dicha norma describe. Y si quien los conserva es un particular, habría que acudir a la habilitación genérica que propone el art. 7.1 de la Ley Orgánica 7/2021, en conjunción con el mandato del art. 575 de la LECRIM[71]. El apartado 2 del citado art. 588 ter j de la LECRIM incluye igualmente en el mismo ámbito a lo que se define como la *búsqueda entrecruzada o inteligente de datos.*

Obviamente, la referencia a la normativa sobre conservación de datos debe entenderse en tanto en cuanto la misma se muestre respetuosa con la marcadamente restrictiva jurisprudencia del TJUE a que antes hemos hecho referencia y al respeto del principio de primacía del Derecho de la Unión. El tratamiento de los datos comerciales habrá de encontrar como referente el mandato del art. 15.1 de la Directiva 2002/58/CE y la cesión de datos conservados por razones de otra índole, incluidos los que lo sean bajo la responsabilidad de particulares, habrá de atender al escrupuloso respeto de las limitaciones al tratamiento impuestas por el RGPD y la Directiva (UE) 2016/680.

La norma, inspirada muy probablemente en el pronunciamiento del Acuerdo del Pleno no jurisdiccional de la Sala 2ª del Tribunal Supremo de 23 de febrero de 2010, somete la medida de injerencia a una estricta reserva de autorización judicial: el juez de instrucción competente. Y en ello, al igual que en un principio pudiera pensarse en cuanto a la delimitación de sujetos obligados y, con matices, como hemos visto, en cuanto respecta a la fuente de conocimiento, garantizará una perfecta sintonía con la jurisprudencia del TJUE. Ello adquiere especial interés cuando se pretende acceder a información que trasciende a la simple aportación de datos sobre quién está detrás de una determinada identidad electrónica o qué identidades tiene registradas a su nombre una determinada persona; que es a lo que se refiere el art. 588 ter m al reconocer en la Policía Judicial y Ministerio Fiscal capacidad para poder solicitar directamente tal información de los correspondientes sujetos obligados. La asociación entre una IP dinámica y el punto de terminación de red no es un dato identitario[72] como tampoco lo es la asociación entre un IMEI y un IMSI. Ambos son datos que trascienden a la simple fina-

exteriorizar en la cabecera IP información visible sobre el verdadero destino. Puede consultarse sobre el particular el interesante trabajo de ORTIZ PRADILLO. Juan Carlos: *"Desafíos legales actuales a la identificación de usuarios de redes TOR"*; en *Curso sobre intervención de comunicaciones telemáticas*, organizado por la Fiscalía General del Estado, Base de Datos del Centro de Estudios Jurídicos del Ministerio de Justicia; 2014.

[71] En este sentido: MONTORO SÁNCHEZ, Juan Alejandro: *"Uso y cesión de datos de carácter personal en el proceso penal"*. Editorial Thomson Reuters- Aranzadi, Pamplona 2022; pág. 344.

[72] Véase sobre el particular la STEDH, Secc. 4ª, de 24 de abril de 2018 (caso BENEDIK v Eslovenia; asunto 62357/14).

lidad de identificar a la persona física o jurídica que está detrás de una identidad electrónica. El dato identitario sería en el primer caso el abonado que tiene contratado determinado acceso a la red o que ha accedido a ésta a través de un determinado punto de terminación de red; y en el segundo, el IMSI correspondiente a la tarjeta SIM, a la vez asociada a un determinado número de abonado.

Surge la polémica sobre las modalidades delictivas que podrían ser susceptibles de permitir una orden de cesión de datos relativos a las comunicaciones electrónicas. El nuevo régimen dibujado por la jurisprudencia del TJUE, en cuanto a la especialmente limitada expansión de regímenes de conservación preventiva de datos, lastra claramente la interpretación del art. 588 ter j de la LECRIM, en cuanto a la referencia que a la LCDCE se hace en el mismo dentro de un concepto estricto de delincuencia grave que marca, a excepción del acceso a información sobre titularidades de tarjetas de telefonía de prepago, el art. 1.1 de dicha norma. En modo alguno podemos interpretar el precepto como una especie de retranqueo táctico del legislador en cuanto al nivel de exigencia en orden a la superación del juicio de proporcionalidad a nivel de definición de tipo penal objeto de investigación. La LCDCE se nutre de ese aliento de garantismo que insufla la LO 13/2015 con la incorporación de los principios rectores del art. 588 bis a y en cierto modo facilita la *codificación* de dicha norma, con su sometimiento a concretas exigencias comunes en orden a la motivación y contenido mínimo de la resolución habilitante, al someterse al mandato del art. 588 bis c de la LECRIM. Pero ello, aparte de que pudiera chocar abiertamente con la restrictiva asunción por el TJUE de tales regímenes legales, así como con las trabas y limitaciones en su aplicación, no representa ninguna claudicación en orden a la exigencia de superación del primer juicio de proporcionalidad, auténtico presupuesto[73], de la exigencia de que sea el investigado un delito grave, tal y como es entendido por el Código Penal y leyes penales especiales; siempre bajo el crisol de la interpretación conforme con el concepto de delincuencia grave o asimilada desarrollado por el Tribunal de Luxemburgo, como seguidamente expondremos.

Como bien es sabido, la Circular de la Fiscalía General del Estado 2/2019, sobre interceptación de comunicaciones telefónicas y telemáticas, se valía como argumento para defender que la norma estaba abierta a la investigación de cualesquiera delitos de la comparativa entre la redacción inicial del precepto en el Anteproyecto de la que fuera la LO 13/2015, donde sí se hacía una mención expresa a la actual redacción del art. 588 bis a, y su redacción definitiva; donde desaparece cualquier referencia a la naturaleza de infracciones penales cuya investigación permitiría acudir a esta fuente. Sin embargo, argumentos de peso se oponen a tal interpretación permitiendo establecer una estrecha relación de este precepto con el art. 588 ter a, como norma que delimita cuáles serían los delitos susceptibles de albergar tales órdenes de cesión de datos. Por una parte, el Preámbulo de la LO 13/2015, mantiene en el párrafo 11 del apartado IV una interpretación auténtica de la *mens legislatoris* que difícilmente puede ser rebatida: "…*su incorporación al proceso solo se autoriza cuando se trate de la investigación de un delito que, por razones vinculadas al principio de proporcionalidad, sea de los que justifican el sacrificio de la inviolabilidad de las comunicaciones".* Pero el argumento sistemático nos lleva exactamente a la misma solución como norma integrada en una sección, la primera, del capítulo V del Título VIII del Libro II de la LECRIM, intitulada clarificadoramente como *Disposiciones generales*. La influencia de la STJUE del caso LA QUADRATURE DU NET y

[73] En este sentido véase RODRÍGUEZ LAINZ, José Luis: *"Necesidades de reconsideración o reforma de la normativa procesal sobre medidas…"*; op. cit.

otros, y más en concreto de la más reciente STJUE del caso SPETSIALIZIRAN NAKAZATELEN SAD no puede sino reforzar este criterio; si tenemos en cuenta que cuando menos la cesión de datos de tráfico o de localización, así como el tratamiento automatizado de éstos, estaría afecta al concepto de lucha contra la delincuencia grave tal y como es entendida por la jurisprudencia del Tribunal de Luxemburgo. Que otros datos relativos a las comunicaciones pudieran, en su caso, permitir una relajación de esta exigencia de gravedad del delito en base a esa escala decreciente que dibujara la sentencia del caso MINISTERIO FISCAL, no afectaría, por otra parte, al rigor de la ley nacional y ello con la sola excepción de datos identitarios con cabida en el art. 588 ter m, cuya posibilidad de cesión por orden de autoridad judicial sería indiscutible, en una norma que sí relaja con claridad las exigencias de cualidad de la infracción criminal objeto de investigación.

Ahora bien, difícilmente puede defenderse, a la luz de la nueva jurisprudencia del TJUE, que la lista de delitos susceptibles de una injerencia sobre comunicaciones electrónicas no haya sufrido alteración alguna en su debida aplicación como consecuencia de la influencia de la doctrina del Alto Tribunal en el campo de la correlación entre el principio de proporcionalidad y la naturaleza del delito en el que pudiera basarse una orden legal de cesión de datos[74]. Siempre desde la necesaria ponderación de la implicación del principio de proporcionalidad en el caso concreto, los delitos de terrorismo y los cometidos en el seno de una organización o grupo criminal, incluidos obviamente la pertenencia a éstos[75], no ofrecerían problema alguno aparente. Sin embargo, el criterio penológico sí chocaría con la realidad de que el Tribunal de Luxemburgo ha preferido basar el criterio de selección de bienes jurídicos protegidos asimilables al concepto de delito grave no tanto en el concepto *ad hoc* de delito grave que se recoge en el art. 579.1.1º. de la LECRIM, sino en bienes jurídicos que, abarcando la salvaguardia de concretos derechos fundamentales garantidos por la CDFUE, han sido considerados dignos de una especial protección. El criterio de la determinación de la gravedad del delito en función de la gravedad de la pena prevista por la norma punitiva solo permitiría, por tanto, una debida ponderación del juicio de proporcionalidad de segundo orden, pero partiría del presupuesto de poder relacionarse el hecho investigado con alguno de esos bienes jurídicos que destaca dicha jurisprudencia, o que pudieran derivarse de las necesidades de protección de otros derechos reconocidos en la CDFUE de similar trascendencia. Con más motivo, el componente instrumental definido en el art. 588 ter a de la LECRIM, los *"delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación"*, difícilmente podrían tener asiento en esa categorización de la delincuencia grave, como no fuera que estuvieran relacionados con la investigación de delitos que pudieran considerarse delincuencia grave o equiparable a ella y ello por mucho que la STC 104/2006, de 3 de abril, llegara a atribuir la condición de nuevo criterio superador del juicio de proporcionalidad a ese componente instrumental de la *potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito.* Como se ve, una interpretación conforme con la jurisprudencia del Tribunal de Luxemburgo del listado de delitos susceptibles de permitir una cesión de datos de tráfico y localización o la búsqueda entrecru-

[74] Seguimos en este punto la tesis desarrollada por RODRÍGUEZ LAINZ, José Luis: *"Necesidades de reconsideración o reforma de la normativa procesal sobre medidas…"*; op. cit.

[75] En contra, la citada Circular de la Fiscalía General del Estado 2/2019 (*"Obsérvese que lo que permite la intervención de las comunicaciones es la investigación de delitos cometidos en el seno de una organización o grupo criminal, no la investigación del propio delito de organización (art. 570 bis CP) o grupo criminal (570 ter CP)"*).

zada e inteligente de datos relativos a las comunicaciones se hace precisa; pero es perfectamente viable.

Esa poderosa fuerza expansiva de los conocidos como principios rectores recogidos en el art. 588 bis a de la LECRIM[76], hace acto de presencia en la redacción del art. 588 ter j de la LECRIM. La propia referencia a la incorporación del material objeto de cesión al proceso es un claro tributo al principio de especialidad de la medida y los principios de idoneidad y necesidad encuentran no una acogida, sino una especial enfatización cuando en el apartado 2 de la norma se nos dice que el conocimiento de estos datos ha de ser *indispensable*, a la vez que en cuanto a la necesidad, asociada al concepto de alcance de la medida -art. 588 bis c.3,c)-, de precisión de *la naturaleza de los datos que hayan de ser conocidos*.

La exigencia del deber de motivación se deriva igualmente del propio mandato del apartado 2 del art. 588 ter j (necesidad de incluir en la resolución autorizante *las razones que justifican la cesión*) en conjunción con el mandato del art. 588 bis c.3, en sus letras a) y c), en cuanto a la debida *expresión de los indicios racionales en los que se funde la medida* y *la motivación relativa al cumplimiento de los principios rectores establecidos en el art. 588 bis a.* Que la jurisprudencia del Tribunal Constitucional, en sus SSTC 123/2002, de 20 de mayo, y 26/2006, de 30 de enero, en base al principio de la menor intensidad de la injerencia, haya permitido una cierta relajación tanto en la acreditación de las exigencias de superación del presupuesto habilitante, como en la ponderación de su contraste con determinados principios rectores, no significa en modo alguno una confrontación con la jurisprudencia más exigente del TJUE. De nuevo una interpretación conforme es posible, y necesitará solo una readaptación a los nuevos parámetros definidos por el Tribunal de Luxemburgo.

La condescendencia del TJUE con regímenes de valoración de la evidencia obtenida por una fuente ilícita, en este caso por contravención de las exigencias de aplicación del art. 15.1 de la Directiva 2002/58/CE, en base a la validación del empleo de la doctrina sobre el llamado principio adversarial, podría encontrar cierto predicamento en la jurisprudencia española. No debe dejarse atrás que la polémica STC, Pleno, 97/2019, volviendo a los postulados que proponía el precedente de la STC 114/1984, 29 de noviembre, muestra su conformidad con la doctrina de la Sala Segunda del Tribunal Supremo que, con punto de arranque en la STS 116/2017, de 23 de febrero, diera carta de naturaleza a la posible valoración de evidencias o fuentes de conocimiento obtenidas por particulares con transgresión de derechos fundamentales, posteriormente seguida por las SSTS 287/2017, de 19 de abril, y 508/2017, de 4 de julio[77]. Dicha doctrina parte como primer criterio de exclusión de esta fuente de conoci-

---

[76] Autores como GARCIMARTÍN MONTERO, Regina ("*Regulación de diligencias tecnológicas en la investigación penal: aciertos y carencias"*; en: *La tecnología y la inteligencia artificial al servicio del proceso*. Editorial COLEX S.L. A Coruña 2023; págs. 166 y ss.), abogan por la necesidad de expandir estos principios rectores a otras diligencias restrictivas de derechos fundamentales; pero la norma no hace sino recoger y hacer explícitos unos principios que ya habían sido debidamente reconocidos tanto por la jurisprudencia de nuestro Tribunal Constitucional como de la Sala Segunda del Tribunal Supremo, en quienes sin duda el legislador se inspira.

[77] Una valoración crítica de la sentencia puede encontrarse en el trabajo de LORCA NAVARRETE, Antonio María., *"La prueba que vulnera derechos fundamentales"* (Revista Vasca de Derecho Procesal y Arbitraje 1 2023, Tomo XXXV); y en general, como más reciente ejemplo de radical oposición a la aplicación en nuestro ordenamiento de la doctrina sobre el efecto disuasorio a GÓMEZ COLOMER, Juan Luis., *"El aumento del intervencionismo público en la investigación del delito"*; en: *La tecnología y la inteligencia artificial al servicio del proceso*. Editorial COLEX S.L. A Coruña 2023; págs. 166 y ss; págs. 181 y 182.

miento de la no consideración de la actuación del particular como encaminada precisamente a obtener, a tal precio, la prueba que pretende oponerse a un tercero, y a quien no le sería de aplicación un efecto disuasorio sí pensado de la actuación de los poderes públicos; al que habría de seguir un segundo juicio, en este caso ponderativo, en el que hubiera de tenerse en cuenta el grado de afectación del derecho fundamental afectado en orden a las necesidades de su tutela constitucional.

Ahora bien, la aplicación que se ha hecho de esta doctrina por el Tribunal Supremo en materia de cesión de datos basados en el mandato de la LCDCE no parte de una vulneración de derechos por parte de un particular, sino de la aplicación de una norma que chocaría frontalmente con las exigencias de los principios de primacía y efectividad del Derecho de la Unión, tal y como han sido entendidos en las sentencias de los casos LA QUADRATURE DU NET y otros y G.D. y AN GARDA SÍOCHÁNA. Por supuesto que las posibilidades de aplicación de criterios de corrección de las llamadas *exclusionary rules*, como sucediera con el hallazgo inevitable en la STC 22/2003, de 10 de febrero, no cierran plenamente las puertas a situaciones en que la transgresión proviniera de la actuación de concretos poderes públicos. De hecho, la doctrina del TEDH sobre el llamado principio adversarial, basada en la realización de un juicio de balance del conjunto probatorio al efecto de determinar si el derecho a un juicio justo se ha respetado en el caso concreto, y que la parte afectada por la medida ha gozado de la posibilidad real de controlar y contradecir la autenticidad y oportunidad del medio probatorio obtenido con contravención de derechos fundamentales[78], no llega a hacer distingos sobre la condición pública o privada del transgresor. Pero el problema radica realmente en que *"…lo que plantea el Tribunal Supremo no es tanto dar una solución concreta sobre la posible utilización procesal de una determinada evidencia como servir de argumento para mantener* [sine die] *la vigencia de la ley nacional"*[79] mantener *sine die* su vigencia. La interpretación, conforme a la doctrina jurisprudencial del TJUE, de las posibilidades de aplicación de la doctrina del TEDH sobre el principio adversarial a la hora de valorar la utilización de datos obtenidos con transgresión del mandato del art. 15.1 de la Directiva 2002/58/CE, debe sobreponerse sin duda a una jurisprudencia nacional que a duras penas puede justificar la inexistencia de un apartamiento del principio de primacía del Derecho de la Unión, y de sus variantes de los principios de equivalencia y efectividad.

Ni que decir tiene que el art. 588 ter m de la LECRIM, en tanto que atribuye a Ministerio Fiscal y Policía Judicial competencia para recabar de prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información determinados datos identitarios relacionados con el concepto de identidad civil, se hace merecedor de un análisis crítico que permita su adaptación a las exigencias de la jurisprudencia del TJUE. En buena parte podríamos aplicar similares conclusiones a las que hemos llegado al analizar brevemente el art. 588 octies de la LECRIM. Pero aquí, la posibilidad de atribución de tal facultad a una autoridad policial o fiscal, y la limitación del control judicial a un nivel en cierto modo residual (solamente cuando la investigación es judicializa-

[78] Como simple ejemplo, en cuanto que relacionado con nuestra jurisprudencia constitucional -STC 142/2012, de 2 de julio-, podríamos citar a la STEDH, Secc. 2ª, de 17 de enero de 2012 (caso ALONY KATE v. España; asunto 5612/08). La sentencia del Tribunal Constitucional aborda un supuesto de acceso por parte de agentes policiales a la agenda y registro de llamadas de teléfono móvil incautado a una sospechosa en un puesto fronterizo.

[79] En este sentido, RODRÍGUEZ LAINZ, José Luis., *"La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada…"*; op. cit.

da, o cuando un ciudadano hace uso de sus derechos de información, oposición o cancelación), encuentran una mejor justificación. Ya hemos anticipado, de hecho, cómo existe cierto grado de condescendencia sobre el particular en la jurisprudencia del TEDH y cómo el TJUE no ha llegado a pronunciarse aún de forma abierta sobre esta posibilidad de que tales autoridades puedan o no recabarlas por sí mismas, sin necesidad de una previa o ulterior autorización o ratificación judicial o de autoridad administrativa independiente.

Un adecuado análisis de la norma nos permite apreciar cómo realmente la norma ofrece más garantías que las que aparenta, aunque sea manifiestamente mejorable en su redacción y técnica normativa.

El reconocimiento de la facultad para recabar directamente los datos de identidad solamente puede ser entendido en el escenario de una concreta investigación criminal. No otro sentido, en el contexto en que está ubicado el precepto, puede darse a la vez *en el ejercicio de sus funciones.* La norma encuentra igualmente un reforzamiento en la competencia y funcionalidad de tal cometido en el art. 7.1 de la Ley Orgánica 7/2021 toda vez que ésta circunscribe tal facultad en el contexto de la *investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas*; y, además, encorseta tal actuación, en cuanto respecta a la actuación propia de la Policía Judicial, en el cometido que le atribuye el art. 549.1 de la Ley Orgánica del Poder Judicial de la *"…averiguación acerca de los responsables y circunstancias de los hechos delictivos y la detención de los primeros"*

Por otra parte el exceso en el recabo de información, aparte de poder incidir directamente en el principio de proporcionalidad, nos llevará a una situación en la que la reserva de autorización judicial se convertiría en un indiscutible fundamento para derivar tal competencia a ésta teniendo en cuenta ese carácter excepcional y claramente subsidiario que se reconoce por nuestra jurisprudencia constitucional a las restricciones de derechos fundamentales por quien no ostenta la cualidad de autoridad judicial[80]. Con más motivo, si se pretende utilizar esa información en procedimientos de búsqueda entrecruzada o inteligente de datos que sería genuina de la autoridad judicial por mandato del art. 588 ter j.2.

La sujeción a los principios rectores de la norma garantizará sin duda alguna la necesidad de que tales decisiones se sometan a los distintos juicios ponderativos que exige dicho precepto. Es cierto que las Circulares de la Fiscalía General del Estado publicadas en interpretación de la LO 13/2015 cuestionaban, en concreto, la aplicación del art. 588 bis a de la LECRIM a las actuaciones policiales. Pero, ni el art. 588 ter m de la LECRIM llega a mostrar una contrariedad implícita ni explícita a la aplicación de dicha norma general, dotada como está de una inusitada fuerza expansiva, ni puede olvidarse que tales principios habrían de informar realmente cualquier actuación de los poderes públicos afectante a derechos fundamentales de las personas. Una tal interpretación pone realmente en riesgo el empleo de tales facultades como vía expedita para prodigar el abuso o arbitrariedad en su empleo máxime si tenemos en cuenta que el control judicial se difuminaba, hasta la entrada en vigor de la LO 7/2021, al albur de una concreta decisión de judicializar la investigación o del ejercicio por personas afectadas de sus derechos relacionados con la protección de sus datos personales. Sería además un contrasentido que el art. 588 bis b.2.2º. sí exija una incontestable sumisión a los principios rectores cuando la autoridad policial o fiscal debe acudir a un juez para la autorización de la medida de investigación tecnológica, mas no para acordarla por sí mismas cuando tienen reconocida como propia tal competencia. Cualquier intento de mantener esa no

[80] Por citar un ejemplo paradigmático, la STC 70/2002, de 3 de abril.

aplicabilidad del art. 588 bis a chocaría con el mandato contenido en el mismo art. 7.1 de la LO 7/2021, en cuanto a que la emisión de una orden de cesión de datos ha de efectuarse siempre *"…de forma motivada, concreta y específica"*. La motivación no solo puede ser entendida en un contexto de cumplimiento de exigencias del presupuesto habilitante; no tiene sentido sino es en cuanto que exigente de que se justifiquen las razones por las que se ha tomado la decisión de afectar, aunque sea de forma tan liviana, a determinados derechos fundamentales.

El último gran obstáculo al que ha de enfrentarnos el art. 588 ter m de la LECRIM, interpretado conjuntamente con el citado art. 7 de la LO 7/2021, es el del cumplimiento del deber de información a las personas afectadas a que se refiere la STJUE de 17 de noviembre de 2022, en base al mandato del art. 13 de la Directiva (UE) 2016/680; lo cual incluiría no solo el acceso de forma efectiva a dicho conocimiento, sino también la apertura de vías de recurso contra el acceso ilícito a tales datos. Dicho precepto, no lo olvidemos, si bien impone al responsable del tratamiento el cumplimiento del deber de información a los interesados cuyos datos han sido objeto de tratamiento, establece, en su apartado 4, la posibilidad de que los Estados miembros adopten medidas legislativas que permitan retrasar, limitar u omitir la puesta a disposición del interesado de la información; en tanto que éstas constituyan una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada y tengan como finalidad, entre otras: evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; o proteger la seguridad pública, la seguridad nacional, o los derechos y libertades de otras personas.

Tal disposición desborda claramente ese peculiar régimen de secreto en la adopción de medidas de investigación tecnológica que se recoge en el art. 588 bis d de la LECRIM; y su posible expansión más allá de la finalización de la ejecución de tales medidas en un contexto de interceptación de comunicaciones electrónicas, pero con potencial expansión a otros supuestos, a que se refiere el art. 588 ter i.3. La norma que sirve de fundamento para esa no inmediata comunicación a los interesados de la existencia de una orden de cesión de datos identitarios acordada por una autoridad policial o fiscal ha de encontrarse en el art. 7.4 de la LO 7/2021. Que en cuanto respecta a las posibles limitaciones, por las mismas razones, en cuanto al ejercicio de los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento, habrá de ser el art. 24.1 aunque en este caso, con exigencia de una debida motivación en la decisión denegatoria del derecho de acceso. Dicho precepto establece una excepción generalizada al deber de información de los supuestos habilitantes del tratamiento sin recabar previo consentimiento del interesado referidos en los apartados anteriores del mismo precepto y esa excepción, que abarca tanto a la autoridad ordenante como al responsable del tratamiento obligado por una orden de cesión de datos, no conoce más límite temporal que el de que se garantice *la actividad investigadora.* La norma solamente podría entenderse, en claro parangón con lo que nos dijera el art. 588 ter i.4 de la LECRIM, en cuanto a la posibilidad de no puesta en conocimiento a los interesados por poder *perjudicar futuras investigaciones* desde luego en un contexto de pervivencia de la necesidad de mantener la discreción de concretas o futuras investigaciones.

Pero el precepto no va más allá de esta referencia genérica a la garantía de la actividad investigadora sin determinar procedimientos realmente eficaces de control por parte de las autoridades judiciales, y haciendo recaer en los ciudadanos buena parte de la carga de hacer valer sus derechos de información, acceso, rectificación, supresión y limitación de su tratamiento, prácticamente a ciegas, o como consecuencia de la judicialización de la investiga-

ción, si es que ésta llega a tener lugar. La propia regulación de las bases de datos policiales, tal y como venía establecido en los arts. 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, donde sí se llegaban a establecer, aunque con cierto grado de relativización, concretos plazos de conservación, nos enfrenta a un preocupante dilema jurídico[81]. Hemos de partir de la base de que la Disposición adicional décimo cuarta de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, garantizaba la vigencia de ambos preceptos, en tanto en cuanto no fueran expresamente modificados, sustituidos o derogados debiendo por ello considerarse implementación del mandato de la Directiva 2016/680/UE, aunque fuera de forma provisional. Pero lo cierto es que la citada LO 7/2021 guarda silencio sobre la vigencia de estas normas; que no necesariamente se contraponen al contenido de la misma. Tampoco su Disposición derogatoria única incluye ninguna mención específica a la derogación de ambos preceptos. Dar una respuesta jurídica incontestable a tal dilema resulta realmente complejo.

La situación es igualmente compleja en el supuesto de decisiones adoptadas por el Ministerio Fiscal al amparo del art. 588 ter m. El apartado tercero del art. 5 de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal, no prevé una puesta en conocimiento de la autoridad judicial de la existencia de decisiones de cesión de datos identitarios en el curso de una investigación preprocesal, más allá de los supuestos en que se decide interponer denuncia o querella criminal. Hemos de acudir nuevamente al art. 7.1 de la LO 7/2021 para encontrar un basamento jurídico de ese deber de comunicación aunque sería recomendable establecer en tales supuestos de archivo un mecanismo de comunicación unido a la definición de las capacidades reales de fiscalización por parte de la autoridad judicial competente, así como eventual capacidad de decisión sobre la no puesta en conocimiento del hecho de la injerencia a las personas interesadas o su dilación en el tiempo, con o sin controles ulteriores en justificación de su mantenimiento.

Las posibilidades de acceso a los recursos efectivos frente a órdenes de cesión o denegación de peticiones de los interesados en relación con el ejercicio de los derechos relacionados con la protección de sus datos personales sí contaría, sin embargo, con un generoso régimen jurídico en el que podrían encontrar respuesta a sus legítimas expectativas. Y ello no solo por la batería de derechos y vías de reclamación que se articulan en la LO 7/2021, sino en cuanto a las posibilidades de actuación derivadas de la judicialización del expediente; y, en concreto por razón de las vías reaccionales que sin duda les ha de abrir el apartado 3 del art. 588 ter j de la LECRIM, como consecuencia de la puesta en conocimiento de la existencia del acto de injerencia.

En definitiva, la necesaria mejora de la legislación española, en cuanto respecta al régimen de cesión de datos establecido por mandato del art. 588 ter m de la LECRIM, debería atender a las siguientes demandas:

1. Sería recomendable establecer un procedimiento de dación de cuenta de tales órdenes de cesión de datos de origen policial y fiscal, determinando el cometido y alcance de la fiscalización de tales medidas por parte de la autoridad judicial; independientemente de la actividad de control que pudiera llevar a afecto la Agencia Española de Protección de Datos como autoridad administrativa independiente.

---

[81] Seguimos en este punto la tesis desarrollada por RODRÍGUEZ LAINZ, José Luis., *"Necesidades de reconsideración o reforma de la normativa procesal sobre medidas…"*; op. cit.

2. Debería clarificarse aún más la determinación de los motivos y plazos durante los cuales puede dilatarse el deber de información a los interesados del hecho mismo de la cesión y tratamiento de sus datos; y en concreto clarificar las dudas sobre la vigencia de la normativa sobre bases de datos policiales a que se refieren los arts. 23 y 24 de la LO 15/1999.

3. Debería determinarse la forma de puesta en conocimiento de la autoridad judicial de aquellas diligencias de investigación tramitadas por el Ministerio Fiscal que no dieran como resultado la interposición de denuncia o querella contra personas determinadas, en las que se hubieran emitido órdenes de cesión de datos en base a lo dispuesto en el art. 588 ter m de la LECRIM.

BIBLIOGRAFÍA UTILIZADA:

BERMEULEN, Judith: *"Bulk retention of private-sector subscriber data for governmental purposes does not violate the Convention: Breyer v. Germany"*; Fuente: https://strasbourgobservers.com/2020/03/05/bulk-retention-of-private-sector-subscriber-data-for-governmental-purposes-does-not-violate-the-convention-breyer-v-germany/

BAHAMONDE BLANCO, Miriam: *"Medidas de investigación tecnológica a la luz de los Derechos Fundamentales, una cuestión pendiente".* Diario La Ley, Nº 9160, Sección Tribuna, 16 de marzo de 2018, Editorial Wolters Kluwer.

BREITENMOSER, Stephan; *"Der schutz del Privatsphäre Gemäs art. 8 EMRK";* Editores Helhing y Lichitenhahn Basilea, 1986.

CABEZUDO RODRÍGUEZ, Nicolás: *"Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal"*; en I Jornada del Boletín del Ministerio de Justicia: Las Reformas del Proceso Penal; Boletín del Ministerio de Justicia, Año LXX, Núm. 2186, febrero 2016.

ENCINAR DEL POZO, Miguel Ángel: "*La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones".* Top Jurídico, Nuevas Tecnologías, octubre 2014. Editorial SEPIN; Referencia: SP/DOCT/18682.

GARCIMARTÍN MONTERO, Regina: "*Regulación de diligencias tecnológicas en la investigación penal: aciertos y carencias"*; en: *La tecnología y la inteligencia artificial al servicio del proceso*. Editorial COLEX S.L. A Coruña 2023.

GÓMEZ COLOMER, juan Luis: *"El aumento del intervencionismo público en la investigación del delito"*; en: *La tecnología y la inteligencia artificial al servicio del proceso*. Editorial COLEX S.L. A Coruña 2023.

LORCA NAVARRETE, Antonio María: *"La prueba que vulnera derechos fundamentales".* Revista Vasca de Derecho Procesal y Arbitraje 1 2023, tomo XXXV.

MARCHENA GÓMEZ, Manuel y GONZÁLEZ-CUÉLLAR SERRANO, Nicolás: *"La reforma de la Ley de Enjuiciamiento Criminal en 2015"*; Ediciones Jurídicas Castillo de Luna; primera edición, Madrid noviembre 2015.

MONTORO SÁNCHEZ, Juan Alejandro: *"Uso y cesión de datos de carácter personal en el proceso penal".* Editorial Thomson Reuters-Aranzadi, Pamplona 2022.

MORENILLA RODRÍGUEZ, José María: *"El respeto a la esfera privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos"*; en *La jurisprudencia del Tribunal Europeo de Derechos Humanos*. Cuadernos de Derecho Judicial. CGPJ, Madrid 1993.

OCÓN GARCÍA, Juan: *"Derecho fundamental al secreto y tecnologías avanzadas de comunicación".* Centro de Estudios Políticos y Constitucionales; Primera Edición. Madrid, 2021; pág. 36.

ORTIZ PRADILLO. Juan Carlos: *"Desafíos legales actuales a la identificación de usuarios de redes TOR"*; en Curso sobre intervención de comunicaciones telemáticas organizado por la Fiscalía General del Estado, Base de Datos del Centro de Estudios Jurídicos del Ministerio de Justicia; 2014.

ORTIZ PRADILLO, Juan Carlos: *"Europa: Auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas".* Revista General de Derecho Procesal 52 (2020).

RODRÍGUEZ LAÍNZ, José Luis: *"La definitiva defenestración de la ley española sobre conservación de datos relativos a las comunicaciones".* Diario La Ley Nº 8901, Sección Doctrina, 16 de enero de 2017. Wolters Kluwer.

RODRÍGUEZ LAÍNZ, José Luis: *"Reflexiones sobre el tratamiento de datos personales por prestadores de servicios de comunicaciones vía internet para la lucha contra abusos sexuales de menores en línea en el Reglamento (UE) 2021/1232".* Diario La Ley, Nº 9974, 20 de diciembre de 2021, Wolters Kluwer.

RODRÍGUEZ LAÍNZ, José Luis: *"La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G.D. y Comissioner an Garda Síochána"*. Diario La Ley, Nº 10058, Sección Tribuna, 28 de abril de 2022, Wolters Kluwer.

RODRÍGUEZ LAÍNZ, José Luis: *"Necesidades de reconsideración o reforma de la normativa procesal sobre medidas de investigación tecnológica"*; en: "Blockchain, inteligencia artificial y criptomonedas en el proceso penal". Colección: Cuadernos Digitales de Formación Nº volumen: 12 Año: 2022. CGPJ.