Foro, Nueva época, vol. 26, núm. 2 (2023): 155-180 ISSN: 1698-5583
https://dx.doi.org/10.5209/foro.97648

LA ORDEN DE PRESESERVACIÓN DE DATOS DEL ART. 588 OCTIES DE LA LEY DE ENJUICIAMIENTO CRIMINAL

José Luis Rodríguez Lainz
Magistrado-Juez Titular del Juzgado
de Instrucción núm. 4 de Córdoba
josel.rodriguez@poderjudicial.es

RESUMEN

El art. 588 octies LECrim ha permitido dotar a Policía Judicial y Ministerio Fiscal de una eficaz herramienta para garantizar evitar la destrucción, borrado o anonimización de datos que pudieran ser cruciales en el contexto de una concreta investigación criminal, a la espera de poderse perfilar la justificación y alcance de una concreta solicitud de autorización de cesión de datos dirigida al juez competente. Sin embargo, una excesiva dependencia del precedente del art. 16 del Convenio Europeo sobre la ciberdelincuencia ha colocado tal regulación, en cuanto respecta a los plazos de conservación, existencia de un control judicial efectivo y definición de las infracciones criminales cuya investigación podría permitir el uso de esta herramienta, en una muy delicada situación respecto de la jurisprudencia tanto del TEDH como del TJUE; que impone una labor de exégesis muy forzada del texto normativo para tratar de conciliar su redacción con las exigencias de aquellas.

Palabras clave: proceso penal, sentencia criminal, Derecho europeo, justicia europea, investigación, cesión de datos.

ABSTRACT

Article 588 of Criminal Procedure Law has made it possible to provide the Judicial Police and the Public Prosecutor's Office with an effective tool to ensure the destruction, deletion or anonymisation of data that could be crucial in the context of a specific criminal investigation, the justification and scope of a specific request for authorization to transfer data addressed to the competent judge being pending. However, an excessive dependence on the likely case law made by article 16 of the European Convention on Cybercrime has placed such regulation, in ter*ms of retention periods, of the existence of effective judicial control and the definition of the criminal offences whose investigation could allow the use of this tool, in a very delicate situation with regard to case law of both the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) which imposes a very forced work of exegesis of the normative text in order to try and reconcile its wording with the requirements of the former.*

Keywords: Criminal procedure, criminal sentence, EU Law, EU Justice, research data transfer.

ZUSAMMENFASSUNG

Der Art. 588 der Strafprozessordnung hat es der Kriminalpolizei und der Staatsanwaltschaft ermöglicht, ein wirksames Instrument zur Verfügung zu stellen, um die Zerstörung, Löschung oder Anonymisierung von Daten zu verhindern, die in einer bestimmten strafrechtlichen Untersuchung von entscheidender Bedeutung sein könnten, während auf die Rechtfertigung und Reichweite eines konkreten Antrags auf Datenübermittlung an den zuständigen Richter gewartet wird. Allerdings hat eine übermäßige Abhängigkeit von der Vorgängervorschrift des Art. 16 des Übereinkommens über Computerkriminalität zu einer sehr prekären Situation dieser Regelung hinsichtlich der Aufbewahrungsfristen, der Existenz einer effektiven gerichtlichen Kontrolle und der Definition der Straftaten geführt, deren Untersuchung den Einsatz dieses Instruments rechtfertigen könnte. Dies erfordert eine sehr anspruchsvolle Auslegung des Gesetzestextes, um dessen Wortlaut mit den Anforderungen des Europäischen Gerichtshofs für Menschenrechte (EGMR) und des Europäischen Gerichtshofs (EuGH) in Einklang zu bringen.

Schlüsselwörter: Strafprozess, Strafurteil, Europäisches Recht, Europäische Justiz, Untersuchung, Datenübermittlung.

I. INTRODUCCIÓN: EL REFERENTE DEL ART. 16 DEL CONVENIO EUROPEO SOBRE LA CIBERDELINCUENCIA

Cuando el legislador decidió abordar la nueva figura de las órdenes de preservación de datos en la Ley Orgánica 13/2015[1] no tuvo el más mínimo reparo en reconocer que la norma nacional se inspiraba en el art. 16 del Convenio Europeo sobre la Ciberdelincuencia de 23 de noviembre de 2001, también conocido como Convenio de Budapest. Tal era su confianza en esa equiparación, que introdujo en el Preámbulo de la Ley Orgánica, apartado III, párrafo 15, la siguiente afirmación: «Esta norma toma como

[1] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

referencia el art. 16 del Convenio sobre la Ciberdelincuencia, de 23 de noviembre de 2001, ratificado por España el 20 de mayo de 2010».

Se trata, como veremos, de una afirmación más que discutible; en la que ese concepto de referente debería ser suplido tal vez por una voz más inespecífica, como pudiera ser la de *inspiración*. Y es que el traslado de un esquema basado en un contexto de cooperación judicial internacional en el ámbito de los datos electrónicos encuentra un no sencillo encaje en el escenario de una actuación de ámbito nacional en la que no existen órganos requirentes ni requeridos, sino diferentes actores de la investigación criminal relacionados con la necesaria ulterior intervención de una autoridad judicial investigadora.

Las denominadas *expedited preservation of stored computer data* nacen en un contexto en el que el redactor del Convenio era consciente de que, con los mecanismos tradicionales de la cooperación judicial internacional, basados en criterios de escrupuloso respeto de la soberanía de los Estados requeridos, cualquier intento serio de cesión de unos datos electrónicos caracterizados por su fugacidad y capacidad de inmediata destrucción, ocultación o borrado, estaba condenado al fracaso. Debía por ello buscarse una solución ágil que permitiera, con respeto del principio de soberanía de los Estados firmantes del Convenio, el buen fin de tal cometido; consiguiéndolo gracias al diseño de una ágil herramienta que permitía, mediante la preservación de los datos en origen por parte de quien los poseyera o tuviera bajo su control, limitar al mínimo indispensable el alcance de la injerencia sobre la protección de datos personales y, por ende, el grado de afectación de la soberanía del Estado requerido.

La desformalización del trámite facilitaba poder acudir a cauces más ágiles de comunicación; pero se establecían plazos perentorios en términos de cooperación judicial internacional, hasta noventa días prorrogables en los términos establecidos en la legislación de cada Estado miembro, para formalizar la petición de cesión de los datos por los cauces tradicionales. Es este un plazo que, pese a que pareciera ser excesivo y desproporcionado en el contexto de rapidez de respuesta en que aparenta darse forma al precepto, se adapta a los ritmos y tempos propios de los protocolos de cooperación judicial internacional.

Pero de ahí a poder importar buena parte del esquema diseñado por el redactor del Convenio para trasladarlo, sin las adecuadas adaptaciones, a un escenario de legislación interna hay un abismo. Quienes están facultados para emitir una tal orden de preservación tienen asumido un cometido específico en la investigación criminal, e intervienen en el procedimiento

de investigación formando parte de engranajes que cuadran perfectamente en una maquinaria investigadora dirigida por quien a la postre ha de asumir la autorización de la orden de cesión de datos cuyo buen fin pretende garantizarse; y se encuentran además no so solo a pocos kilómetros o metros de distancia de este último, sino bajo el amparo de una misma norma procesal.

Un avezado lector de la norma nacional seguramente habrá apreciado cómo he preferido usar la voz *preservación* en vez de la de *conservación* que intitula al art. 588 octies LECrim. Aparte de hacer propia la expresión que es utilizada en el Convenio de Budapest, encuentro razones metodológicas que me llevan a preterir la voz empleada por el legislador nacional frente a esta. Razones metodológicas, de permitir distinguir esta figura respecto de otras con las que muestra cierto grado de parentesco, y que utilizan la misma voz *conservación de datos.*

Hemos de distinguir en primer lugar la orden de preservación de la *conservación generalizada e indiscriminada de datos,* según la denominación que fuera en primer lugar acuñada por la STJUE (Gran Sala) de 21 de diciembre de 2016 (caso *Tele2 Sverige AB y otros,* asuntos C203/15 y C698/15); es decir: aquellas obligaciones de conservación con origen en la defenestrada Directiva 2006/24/CE[2], o en la normativa nacional de desarrollo[3]. En este supuesto, es la propia ley, completamente ajena a cualquier forma de decisión de autoridad pública, quien impone a los destinatarios de la norma la obligación de conservar miles de millones de datos relacionados con la prestación de servicios de comunicaciones electrónicas, durante determinados periodos de tiempo. La finalidad de estas bases de datos atendería no ya a criterios de probabilidad, sino de posibilidad de una hipotética futura utilización procesal a modo de petición de cesión de datos derivada de una investigación criminal o para concretas necesidades relacionadas con la seguridad nacional.

La misma sentencia del caso *Tele2 Sverige AB y otros* modeló otras dos formas de conservación o retención, una generalizada y otra marcadamente selectiva de datos; desarrollándose de forma más extensa en la posterior

---

[2] 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. Como bien es sabido, la Directiva fue declarada inválida por 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).

[3] En nuestro caso, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

STJUE (Gran Sala) de 6 de octubre de 2020 (caso *La Quadrature du Net y otros,* asuntos C-511, 512 y 520/18).

En la primera de ellas, y a los solos efectos de salvaguardia de la seguridad nacional, aunque la decisión parte del presupuesto de la existencia de una norma con forma de ley habilitante, la responsabilidad en su emisión competería a una concreta autoridad judicial, u otra autoridad judicial pública independiente, o bajo el control y supervisión de autoridad judicial o administrativa independiente. Pero la propia peculiaridad de esta forma de conservación de datos, referidos en todo caso a medidas restrictivas de derechos relacionados con los derechos protegidos por el art. 15.1 de la Directiva 2002/58/CE[4] (contenidos y datos relativos a comunicaciones electrónicas o de *servicios de comunicaciones interpersonales independientes de la numeración*[5], así como datos de localización accesorios o distintos a los de tráfico), se vería adicionada con la exigencia de que la medida se dirija a hacer frente a una amenaza grave para la seguridad nacional que resulte real y actual o previsible. No existe una correlación perfecta entre los datos cuya conservación se ordena y su ulterior utilización; pero en este supuesto sí se parte de una probabilidad o predictividad de ulterior utilización para su examen, incluso empleando técnicas de injerencia masiva o *bulk interception*, en atención a esa concreta finalidad de salvaguardia de la seguridad nacional con que fuera diseñada la medida.

La segunda modalidad de conservación, más bien retención, afectaría a datos comunicaciones conservados por las operadoras por distintos motivos; permitiendo lo que sería una auténtica retención en este caso sí selectiva, de estos datos, pero en concreto solamente de tráfico o de localización de comunicaciones, siempre que su alcance estuviera delimitado sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico[6], para un periodo temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse. La medida no se reservaría en este caso solo para la pro-

[4] 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).

[5] Adicionados estos al régimen de la Directiva 2002/58/CE por la 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.

[6] La versión de esta herramienta en la STJUE del caso *Tele2 Sverige AB y otros,* incluía otros criterios delimitadores, tales como criterios objetivos o teleológicos; a la vez que la conjunción de unos y otros.

tección de la seguridad nacional, sino que podría ampliarse a la lucha contra la delincuencia grave o amenazas graves contra la seguridad pública. Sí coincidiría su necesaria singularización y la intervención de autoridad judicial o administrativa independiente en su emisión o ratificación y control. La finalidad preventiva, que admitiría tanto datos de pasado como afectantes en una proyección temporal definida, conviviría con una posible utilización concreta en el curso de una investigación criminal ya abierta[7].

Por el contrario, la orden de preservación de datos es por definición selectiva e individualizada; pues atañe a datos que se relacionan con una finalidad específica en el curso de una investigación criminal o una concreta necesidad de la seguridad nacional. Se caracteriza, además, por la urgencia y necesidad en su adopción, hasta el punto de postergar para un momento posterior la petición de una solicitud de cesión de datos a la que se anticipa; y si bien no se exige una perfecta correlación entre lo que se ordena sea preservado y lo que finalmente se solicita a la autoridad judicial, encuentra precisamente su razón de ser exclusivamente en esa concreta finalidad investigadora que la justifica. Existe por ello una estrecha relación entre la orden de preservación y la ulterior solicitud de emisión de orden de cesión de datos.

II. ANÁLISIS DEL ART. 588 OCTIES LECRIM

Ya hemos indicado cómo el art. 588 octies LECrim aprovecha buena parte de la estructura del art. 16 del Convenio de Budapest para dar contenido a esta novedosa institución procesal que hasta entonces solamente podría haber tenido cabida en nuestro ordenamiento procesal en el tan omnipresente art. 13 LECrim. Es este un hecho innegable; y basta comparar ambas normas para comprobar cómo el mimetismo llega tanto desde el empleo de idénticas o similares palabras o frases, hasta la asunción de similares soluciones u opciones jurídicas.

---

[7] Piénsese en el supuesto de investigación de una organización criminal dedicada al tráfico de hachís a través del Estrecho de Gibraltar; en el que hay constancia de que quienes intervienen en los distintos roles de transportistas, receptores de alijos y vigilantes se intercomunican y coordinan empleando teléfonos móviles. La orden de conservación afectante al área geográfica donde se mueve la organización podría interesar tanto a los datos generados en periodos de tiempo anteriores a su comisión como su proyección durante el tiempo de vigencia de la medida. Debe advertirse, sin embargo, que la ausencia de una cobertura legal clara a este tipo de medidas podría condicionar seriamente la posibilidad de dar forma a estas medidas de investigación tecnológica en nuestro ordenamiento procesal.

Surge, sin embargo, la duda sobre si la orden de preservación debe o no verse sometida a las reglas generales contenidas en el Capítulo IV del Título VIII del Libro II de la LECrim, donde se da contenido a las llamadas disposiciones comunes a las medidas de investigación tecnológica; toda vez que, como apunta la Circular 1/2019 de la Fiscalía General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal (CFGE 1/2019), el art. 588 octies está residenciado en un título distinto, el X; aunque abogue por la expansión de las exigencias propias de los llamados principios rectores como inspiradores de la novedosa institución procesal.

Desde el punto de vista de los antecedentes históricos de la norma, hemos de destacar cómo, efectivamente, la propia idea de introducir en el articulado de la que sería finalmente la LO 13/2015 es realmente tardía. No aparecerá sino en el texto definitivo del Proyecto de Ley Orgánica; y ello desdibuja realmente cualquier intento de encontrar una lógica incontestable en la propia decisión del redactor de la norma de desvincular formalmente a la orden de preservación del resto de las medidas de investigación tecnológica. Pero de ahí a pretender, como prácticamente defiende la CFGE, conferir un carácter neutro, incapaz de afectar a derecho constitucional alguno, a la orden de preservación, prácticamente degradándola a una especie de *diligencias preliminares* al más puro estilo de la Ley de Enjuiciamiento Civil, hay un abismo.

Los vínculos de funcionalidad y teleología con determinadas medidas de investigación tecnológica a las que atiende la orden de preservación, que incluso se ven reflejados en la referencia que se hace en el último inciso del apartado primero del art. 588 octies («... para su cesión con arreglo a lo dispuesto en los artículos precedentes»), son tales que carecería de sentido no establecer un vínculo estrecho entre las disposiciones comunes del Capítulo IV del Título IX y este precepto. La mayor parte de los preceptos de este capítulo nutren de contenido a unos silencios del art. 588 octies que encuentran por razón de ser la circunstancia de que la preservación es preambular a la adopción de concretas medidas de investigación tecnológica; y que en buena parte no hacen sino anticipar parte de su contenido decisor mediante la garantía de que los datos a los que abarca no podrán ser borrados o alterados hasta que la autoridad judicial se pronuncie sobre su cesión o transcurran los plazos de duración de la medida. Relacionar el art. 588 octies con los principios rectores del art. 588 bis *a);* con el contenido motivador de lo que sería la decisión policial o fiscal y su correlación

con el contenido de la decisión judicial —arts. 588 bis *b)* y 588 bis *c)*—; carácter secreto de la decisión más allá de la obligación del sujeto pasivo de la medida —art. 588 bis *d)*—; duración de la medida —art. 588 bis *e)*—; posibilidad de sometimiento a control judicial —art. 588 bis *g)*—; afectación a terceras personas —art. 588 bis *h)*—; cese de la medida —art. 588 bis *j)*—, y destrucción en su caso de los registros —art. 588 bis *k)*—, se convierte en una auténtica necesidad jurídica para copar las exigencias de calidad de la norma habilitante. Resulta realmente difícil dar forma a esta técnica de investigación tecnológica, que lo es como preambular o parte esencial de la orden de cesión, si no es acudiendo a la fuente de unos principios y reglas comunes que la nutren de contenido jurídico.

La norma atribuye la potestad de emitir órdenes de preservación de datos al Ministerio Fiscal y Policía Judicial. Nada se dice sobre la posibilidad de que fuera un juez de instrucción quien emitiera la orden; pero ello no significa en modo alguno que no pudiera hacerlo. De hecho, el empleo de esta herramienta podría resultar especialmente útil como forma de asegurar el sentido de una concreta orden de cesión de datos; aminorando de este modo el espectro de datos o personas afectadas por la medida, a la luz de la información obtenida ulteriormente en el curso de la investigación. Por poner un ejemplo: se garantiza con la decisión judicial de preservación el no borrado de datos de localización de terminales de telefonía móvil que interactuaran con una estación de telefonía BTS en un margen de tiempo de una hora en que se cometió en su área de influencia un homicidio; y una vez seleccionados por otras vías de investigación los posibles autores, se recaba información concreta sobre si sus terminales móviles coinciden con ese criterio de geolocalización. La misma decisión policial o fiscal puede atender a la estrategia procesal del juez instructor; con el beneficio que comporta la reducción del impacto sobre derechos fundamentales de centenares de personas cuyos datos deberían ser objeto de un tratamiento prospectivo.

Aunque la norma no dice nada al respecto, es evidente que la decisión de preservación de datos debe tener una relación directa con una concreta investigación criminal a cargo de la correspondiente autoridad policial o fiscal. No otro sentido puede tener a este respecto la referencia que se hace al final del párrafo primero del art. 588 octies a la formalización de la correspondiente solicitud de cesión de datos a la autoridad judicial.

Los destinatarios del deber de colaboración no son prestadores de servicios de comunicaciones o proveedores de Internet, sino cualquier persona física o jurídica que tenga una concreta relación con los datos cuya preservación se pretende. Debe tenerse muy en cuenta que la norma va

mucho más allá de lo que pudieran considerarse datos relacionados con las comunicaciones electrónicas; que es el soporte informático en el que se conservan los datos interesados el que define realmente el sentido de la orden de preservación. De ahí que haya de precisarse el alcance universal de tal deber de colaboración.

Como consecuencia de la existencia de este deber de colaboración, la norma nos recuerda implícitamente la existencia de otros deberes que, en términos generales, ya se establecían en el art. 588 bis *c).3.h)* LECrim: La colaboración incluye un deber de guardar secreto que, además, viene impuesto con carácter genérico en el art. 588 bis *d)*. Curiosamente, la norma prefiere hacer antes referencia expresa al art. 588 ter *e).3* que al anterior precepto, para introducir la admonición al sujeto obligado de poder incurrir en delito de desobediencia si no cumple con ambos cometidos.

La norma guarda silencio sobre la posibilidad de reconocimiento de excepciones al deber de colaboración, basadas en la relación del secreto profesional, relación familiar o consideración del sujeto obligado como persona investigada en la causa penal; como sí sucede, en concreto, en el supuesto del registro físico o remoto de dispositivos de almacenamiento masivo de datos recogidos en los arts. 588 sexies *c).5*, párrafo segundo y 588 septies *b).2*, párrafo segundo LECrim. Aparte de que una orden de preservación podría tener su razón de ser no solo en cuanto a una ulterior solicitud de orden de cesión de datos, sino también respecto de un registro físico o remoto, cuando la medida pretendiera alcanzar a datos que, pese a estar almacenados en otro sistema informático, pudieran ser lícitamente accesibles por medio del sistema inicial o estuvieran disponibles para este —arts. 588 sexies.*c).3* y 588 septies.3—, no podemos olvidar que al menos la existencia de vínculos de secreto profesional del colaborador podría condicionar la existencia de causas obstativas al cumplimiento de la orden; y que, obviamente, no podría imponerse a un investigado un deber de preservar los datos a su disposición para ser usados en su contra. Tampoco se previene cauce concreto para hacer valer la existencia de motivos obstativos al cumplimiento de la orden, como pudieran ser no solo los ya apuntados, sino también el sometimiento del sujeto obligado a otra jurisdicción nacional o la excesividad de la carga que se le impone. Bastará con la posibilidad de permitirle hacer alegaciones sobre el particular; y, en caso de ser rechazadas, acudir a la correspondiente vía de recurso[8].

[8] El Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación

Son objeto de una orden de preservación datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a disposición de los destinatarios de la orden. La responsabilidad que deben asumir, su conservación y protección hasta que se decida lo procedente sobre la correspondiente orden de cesión o transcurran los noventa días del plazo ordinario o, en su caso, los de su prórroga. No se establece, sin embargo, protocolo alguno sobre la forma en que los sujetos obligados han de asumir tal deber. Es una obligación de resultado, en la que el sujeto obligado debería adoptar las cautelas que tuviera a su alcance; toda vez que es él quien continuará en la posesión exclusiva de los datos, no la autoridad solicitante. Sin embargo, nada debería obstar a que, junto con la orden de preservación, se establecieran directrices (por ejemplo, realización de una copia de seguridad en soporte externo), o incluso facilitarse los medios para que tales cautelas pudieran ser llevadas a efecto (facilitación de herramientas o procedimientos para que la información fuera aislada y conservada con un código hash que asegurara la inexistencia de ninguna forma de cambio o manipulación en la información sometida a preservación).

La norma no establece absolutamente nada sobre la forma y motivación de las resoluciones que acordaran una preservación de datos por parte de autoridad fiscal o policial. Es algo que se sobreentiende sin duda respecto de la autoridad fiscal, pero que es consecuencia del mandato del art. 7.1 de la 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; precepto en el que el deber de motivación de órdenes de cesión de datos o emisión de informes directamente dictadas por autoridades policiales viene expresamente recogido. Pero está claro que la propia indiscutible penetración de los principios rectores en esta medida de investigación tecnológica, y la vinculación a ese contenido mínimo motivador de la decisión que queda perfectamente reflejada en el art. 588 bis *b)*.2.2.º LECrim, harían preciso que la decisión policial, aun en ese contexto de extrema urgencia en el que habitualmente habrán de tomarse estas decisiones, se encuentre soportada por una mínima motivación.

Existe, además, una necesaria relación de congruencia entre aquel contenido sobre el que se impone el deber de preservación y lo que ha de

---

a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales, prevé precisamente vías para plantear objeciones a una orden de cesión de datos cuando la misma adquiere una dimensión transnacional.

solicitarse a una autoridad judicial a modo de orden de cesión o como contenido de una solitud de registro ampliado. Y ello ha de suponer el cumplimiento de una sencilla regla: No se puede acordar la preservación de aquellos datos respecto de los que no existiera una expectativa jurídica razonable de que podrían ser objeto de autorización judicial en cuanto al acceso a su contenido. Y ello solamente puede concebirse desde la perspectiva de un juicio ponderativo que habría de tener un mínimo reflejo en la decisión adoptada por la autoridad policial o fiscal. Ahora bien, sí tendrá razón de ser la mayor extensión del alcance de la medida tal y como se diseña en la decisión de preservación, que lo que definitivamente se solicite a la autoridad judicial, cuando la preservación encuentra una finalidad preventiva; en contextos en los que la perfilación no solo de posibles sospechosos, sino del objeto mismo de lo que se pretende averiguar, es en sí misma difusa y hay riesgo de inminente destrucción, borrado o anominización de los datos.

Sin embargo, la plausible oportunidad del legislador a la hora de dar forma a esta peculiar medida de investigación tecnológica, consistente en afianzar la ulterior disponibilidad de determinadas evidencias o fuentes de información, decae, hasta el punto de comprometer su propia conformidad con las exigencias derivadas de la jurisprudencia de los Tribunales Europeo de Derechos Humanos y de Justicia de la Unión Europea, frente al tratamiento que se hace de dos componentes esenciales de esta herramienta de investigación criminal: Por una parte la excesiva laxitud en la duración de la medida hasta que tiene lugar su judicialización; por otra, el diseño de la intervención de la autoridad judicial en el trasunto de su adopción por autoridad competente hasta la oportuna petición de autorización judicial, si es que tienen lugar.

Importar de una forma tan acrítica los plazos de duración de las órdenes de preservación del art. 16 del Convenio de Budapest ha supuesto un craso error por parte del legislador. Conceder un plazo inicial de noventa días para remitir la solicitud de la correspondiente orden de cesión de datos a la autoridad judicial es, simplemente, una decisión desproporcionada de base. Nada tiene que ver el tiempo preciso para activar una petición de cooperación judicial internacional para obtener la correspondiente cesión de los datos que previamente han sido preservados, con el tiempo que requiere una autoridad policial o fiscal, dentro de sus funciones investigadoras, para recabar la oportuna autorización judicial. Es cierto que en ocasiones la necesidad de una ulterior labor de selección de cuáles son los datos que en concreto han de ser objeto de petición de cesión requiere

de un previo razonable espacio de tiempo; pero, aun así, sigue siendo un plazo excesivo en el que el control judicial sería claramente deficitario, si no inexistente. Lo sencillo habría sido, mantener bajo la reserva de autorización judicial la misma medida de preservación, aunque con posibilidad abierta de su anticipación por autoridades policiales o fiscales a la espera de una ulterior ratificación de la medida; o, cuando menos, involucrar a la autoridad judicial en la posible concesión de prórrogas a un plazo inicial no tan ambicioso. Sin embargo, se ha establecido un peculiar régimen en el que la ausencia de un control judicial efectivo de la medida, como seguidamente veremos, se ve seriamente lastrada por amplios espacios temporales de hasta ciento ochenta días.

La literalidad del precepto impide apreciar la existencia de cualquier forma de control judicial a una decisión de preservación de datos de origen policial o fiscal, como no fuera mediante la presentación de la solicitud de orden de cesión de datos al juez de instrucción competente. Aparte de ello, la LECrim solo se mostraría abierta a una permeabilidad al conocimiento judicial de la decisión de emisión de una orden de preservación del art. 588 octies LECrim en tanto en cuanto se recibiera la una denuncia o querella del Ministerio Fiscal —artículo quinto, apartado tres, de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal—[9] o atestado policial con resultados positivos; o al menos, tratándose de una decisión de archivo, que fuera respecto de aquellas infracciones criminales que, conforme al art. 284.2 LECrim en todo caso deben ser puestas en conocimiento de la autoridad judicial mediante la remisión del atestado practicado.

La propia no reserva de autorización judicial y, obviamente, esta innecesaria desjudicialización de la existencia y vicisitudes de la orden de preservación que regula el art. 588 octies LECrim, podrían encontrar su razón de ser en el escaso nivel de injerencia sobre derechos fundamentales que está detrás de una tal decisión. No es que, al contrario de lo que sostiene la CFGE 1/2019, no se esté afectando a derecho fundamental alguno[10], sino que la incidencia es escasa, enfrentándonos a un claro supues-

[9] «Transcurrido el oportuno plazo, si la investigación hubiera evidenciado hechos de significación penal y sea cual fuese el estado de las diligencias, el Fiscal procederá a su judicialización, formulando al efecto la oportuna denuncia o querella, a menos que resultara procedente su archivo».

[10] De hecho, puede leerse en el apartado 3 de la Circular lo siguiente: «La orden de conservación, en sí misma, no limita derecho fundamental alguno, ya que su único efecto es la "congelación" de los datos ya almacenados, sin que permita el acceso a los mismos cuando se trate de datos íntimos o restringidos».

to en el que, al menos a nivel constitucional, se podría aplicar el principio de la menor intensidad de la injerencia como justificador de la excepción a la reserva de autorización judicial propia de cualquier decisión afectante a los derechos fundamentales de las personas[11]. Cualquier forma de congelación o preservación de datos representa, cuando menos, una somera afectación a determinados derechos relacionados con la protección de datos personales, con amparo en el art. 18.4 de la Constitución Española. Estaríamos hablando, en concreto, de una simple suspensión temporal del principio de funcionalidad en la conservación de datos de carácter personal por quien estaba legitimado a tratarlos con motivo de la prestación de un servicio de telecomunicaciones o cualquier otro servicio que habilitara a su conservación y tratamiento; y a su vez una prohibición de destrucción o eliminación de los datos en cuestión, cuando de particulares se tratara. Realmente esta medida, acordada a expensas de una ulterior autorización judicial de cesión de datos, no llega a afectar de forma directa al núcleo esencial de concretos derechos fundamentales; pero sí les incumbe. Y es evidente que una injustificada emisión de una orden policial o fiscal de conservación al amparo del mencionado precepto sí podría llegar a tener una relevancia a efectos del control constitucionalidad de la medida afectada.

Sin embargo, el impacto de la Ley Orgánica 7/2021, y, en concreto, de su art. 7.1, párrafo primero, ha supuesto un radical cambio en tan preocupante escenario jurídico; en tanto que no solo impone la obligación de motivación de decisiones tomadas por Policía Judicial o Ministerio Fiscal sobre acceso a determinados datos personales no requeridos en su procura de una previa autorización judicial, sino que se exigirá en cualquier caso dar cuenta de la decisión a la autoridad judicial y fiscal[12]. La dación de cuenta se convierte de este modo en insoslayable; y con ello la posibilidad de un mejor control judicial.

Un avezado lector del precepto podría objetar cómo la norma afectaría tan solo a las órdenes de cesión de *datos, informes, antecedentes y jus-*

---

[11] *Vid.* en este sentido, por poner un ejemplo, la STC 70/2002, de 4 de abril.

[12] «Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el art. 549.1 de la Ley Orgánica 6/1985, de 1 de julio y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal».

tificantes; que no a una simple orden de preservación. Pero no hemos de olvidar que los arts. 4 del Reglamento (UE) 2016/679[13] y 3 de la Directiva (UE) 2916/680[14] consideran ya tratamiento la simple conservación de concretos datos personales; requeridos, por tanto, en cuanto a la posible decisión que así lo impusiera de un régimen equiparable al de las órdenes de cesión en sentido estricto. Además, como seguidamente veremos, esta interpretación laxa de la norma es la única que nos permitiría afrontar el duro reto que supone la superación de los presupuestos del control de calidad de la norma habilitante que, en concreto, impone la jurisprudencia del TEDH.

El principio de la calidad de la norma habilitante, que nace en torno a la aplicación por el TEDH del mandato del art. 8.2 CEDH, parte de la exigencia de una ley habilitante previa que regule el supuesto con el suficiente detalle la medida, de modo que se haga cognoscible a cualquier ciudadano, aunque baste para ello con una adecuada indicación de las circunstancias en las cuales y las condiciones bajo las que las autoridades públicas están facultadas a llevarla a efecto[15]; a lo que se añade la superación de unos principios de proporcionalidad y necesidad en el contexto de una sociedad democrática ya en sede de la propia definición normativa. Pero, además, se requiere destacadamente que el propio diseño de la norma garantice que su uso no pueda llevarnos a situaciones de abuso o arbitrariedad[16].

Un sistema de dación de cuenta debería poder suplir esa opción por la autorización judicial como vía más adecuada para proteger la medida de

---

[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.

[15] En este sentido, la Resolución de inadmisibilidad de 29 de junio de 2006 [caso *Weber y Saravia v. Alemania* (asunto 54934/00)], y SSTEDH, Secc. 4.ª, de 18 de mayo de 2010 (caso *Kennedy v. Reino Unido,* asunto 26839/05); Gran Sala, de 4 de diciembre de 2015 (caso *Roman Zakharov v. Rusia,* asunto 47143/06), o, Secc. 2.ª, de 28 de mayo de 2019 (caso *LIBLIK y otros v. Estonia,* asuntos 173/15 y cinco más).

[16] La STEDH, Secc. 4.ª, de 11 de enero de 2022 (caso *Ekimdzhiev y otros v. Bulgaria,* asunto 70078/12) va incluso más allá de la literalidad de la norma, y llega a adentrarse en las consecuencias mismas de su aplicación, para contrastar si los mecanismos de control y garantías con que cuenta son realmente eficaces para tal finalidad de evitación de riesgos de abuso o arbitrariedad.

cualquier atisbo de abuso o arbitrariedad. Pero la misma jurisprudencia del TEDH nos previene de considerar tal puesta en conocimiento como simple plácet o toma en consideración vacuos de cualquier contenido fiscalizador de la decisión adoptada por una autoridad administrativa o fiscal. Siguiendo el ejemplo de las interesantes SSTEDH, Secc. 4.ª, de 2 de diciembre de 2014 (caso *Taraneks v. Letonia,* asunto 3082/06), y, Secc. 4.ª, 16 de febrero de 2016 (caso *Govedarski v. Bulgaria,* asunto 34957/12), tal posición de la autoridad judicial debe someter la medida acordada o anticipada a un doble juicio de valor: En primer lugar, un control de oportunidad; es decir, si la medida era urgente y resultaba procedente la anticipación sin acudir previa o directamente a una autorización judicial. En segundo lugar, un juicio de procedencia y superación de los principios rectores de cualquier injerencia tecnológica, en la que el juez habría de valorar no si de habérsele planteado a él la solicitud habría accedido a la misma, sino realizar un control de los argumentos esgrimidos en la orden emitida o su justificación[17].

El art. 7.1 de la LO 7/2021 no establece ninguna forma de control concreto como consecuencia de la debida comunicación de actos de injerencia sobre datos personales acorados por autoridades policiales o fiscales; tampoco la autoridad judicial competente para recibir tal información. Sin embargo, es evidente que esta información permitiría a la autoridad judicial fiscalizar su contenido; y en caso de encontrar objeciones sobre la propia oportunidad o fundabilidad jurídica de la decisión comunicada, acordar lo procedente para la restauración del orden jurídico aparentemente vulnerado. No otro sentido puede tener este deber de puesta en conocimiento; y de este modo estaríamos salvando la propia conformidad con tal doctrina del TEDH de normas españolas que, como los arts. 588 octies o 588 ter.*m)* LECrim, se abren a la posibilidad de decisiones policiales o fiscales afectantes a ámbitos propios de la protección de datos personales. Debe forzarse para ello la interpretación de la norma nacional y, a la vez, encontrar soluciones jurídicas para darle forma; pero es un tributo que hemos de pagar si es que queremos conciliar tales preceptos con el mandato del art. 8.2 CEDH.

Al menos en mi opinión, es evidente que, en orden a dar forma a estas medidas de preservación de utilidad procesal incontestable, habría resul-

[17] Ambas sentencias hablan de un supuesto de anticipación a una decisión judicial que había de ratificar una decisión policial o fiscal; pero dada su trascendencia como forma de control efectivo frente a riesgos de abuso u arbitrariedad en el ejercicio de la facultad, es evidente que las mismas exigencias, *mutatis mutandis*, son perfectamente exportables al supuesto de simple puesta en conocimiento.

tado conveniente partir de la base de que se definiera la orden de preservación como una anticipación de la decisión judicial con el mismo sentido, requerida de ratificación; ello al menos en aquellos supuestos en que los datos que hubieran de solicitarse estuvieran sometidos a una indiscutible reserva de autorización judicial. En aquellos supuestos en que la autoridad policial o fiscal ejercieran una competencia propia en cuanto al contenido de aquello que pudiera ser objeto de una ulterior orden de cesión no precisada de autorización judicial, la opción por la puesta en conocimiento tanto de la decisión de preservación como de la misma orden de cesión, con posibilidad real de cuestionamiento de la medida por la autoridad judicial, podría mostrarse suficiente a esos efectos de evitación de riesgos de abuso o arbitrariedad.

III. LAS *QUICK FREEZING ORDERS* EN LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

1. Las *quick freezing orders* y su origen jurisprudencial en el Derecho de la Unión Europea

El radical impacto de la STJUE del caso *La Quadrature du Net y otros* sobre concretas medidas de investigación tecnológica tuvo también su reflejo en las que se definieran por dicha sentencia como *quick freezing orders.* Pero no debemos olvidar que esta sentencia y las que le siguieran, en concreto, la STJUE (Gran Sala), de 5 de abril de 2022 (caso *G. D. y Comissioner An Garda Síochána,* asunto C-140/20), no van más allá de los supuestos sometidos a la disciplina del art. 15.1 de la Directiva 2002/58/CE[18]; es decir, como anticipamos anteriormente: Datos relativos a las comunicaciones, incluidos los de tráfico, así como datos de localización asociados a estos o destinados a la prestación de servicios con valor añadido[19]; sometidos como tales a criterios de funcionalidad en su tratamiento

[18] He preferido no abordar el tratamiento de las órdenes europeas de conservación conforme al Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, teniendo en cuenta que la entrada en vigor del Reglamento se ha dilatado hasta el 18 de agosto de 2026; fecha en la que no solo muy probablemente las herramientas de investigación tecnológica que se diseñan por el legislador europeo sean ya obsoletas, sino que podrían ser sujetas a relevantes modificaciones por normas posteriores.

[19] 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 fac-

y deber de destrucción o de conversión en anónimos una vez desaparecida su funcionalidad o necesidades propias de facturación de los servicios prestados a los usuarios, en los términos definidos en los arts. 6 y 9 de la Directiva.

La delimitación del sujeto obligado limitaba aún más el alcance de esta posición jurisprudencial. El art. 15.1 de la referida Directiva restringe su aplicación a los datos tratados por prestadores de servicios de redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público, así como a los prestadores de servicios de la sociedad de la información que presten en concreto servicios de comunicaciones interpersonales independientes de la numeración[20].

La sentencia huye abiertamente de cualquier interpretación que permitiera aplicar un a modo de principio de menor intensidad de la injerencia; y lo hace hasta el punto de equiparar tal nivel de intensidad con el que sería el propio de la ulterior decisión sobre la cesión de datos a la que se anticipa. Tan grave sería, por tanto, la afectación de la protección de datos de tráfico o de localización en un escenario de conservación rápida como la ulterior cesión de los datos preservados a la autoridad solicitante. Y ello traerá sus consecuencias, en orden a imponerse la reserva de este tipo de medidas para la salvaguardia de la seguridad nacional o la lucha contra la delincuencia grave, a cuyo concepto dedicaremos el siguiente apartado de este trabajo a modo de apéndice, así como la reserva de autorización judicial.

Ambas sentencias no se pronuncian con claridad sobre que una orden de preservación de datos solamente pudiera ser emitida por una autori-

---

turación». 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.

[20] En este sentido, la 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 expande el ámbito de aplicación de la Directiva 2002/58/CE a estos; poniéndose como ejemplo en su Considerando 7 el *correo web* y *los servicios de mensajería*. Por su parte, la STJUE del caso *La Quadrature du Net y otros,* 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 2002/58/CE. Ello incluiría, sin duda, a los *servicios de mensajería en Internet*, nos dirá el parágrafo siguiente.

dad judicial. Cuando la sentencia del caso *G. D. y Comissioner An Garda Síochána* se pronuncia sobre la conformidad con el derecho de la unión de tales regímenes, especifica que estos requerimientos a los proveedores de servicios de comunicaciones electrónica han de serlo «... mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo». El control jurisdiccional, sin embargo, es equiparado con el de una autoridad administrativa independiente; y ello excluiría el cometido del Ministerio Fiscal, incluso cuando interviniera en una función directora de una investigación criminal. De hecho, ya desde la citada sentencia del caso *Tele2 Sverige AB y otros* se anticiparía la no consideración de autoridad ni judicial ni administrativa independiente del Ministerio Fiscal, en cuanto respecta en concreto a la cesión de datos relativos a comunicaciones; y la sentencia sería seguida por las SSTJUE de los casos *La Quadrature du Net y otros* y *G. D. y Comissioner An Garda Síochána,* y más en concreto por la STJUE (Gran Sala) de 2 de marzo de 2021 (caso *Prokuratur,* asunto C-746/18) o la más reciente STJUE (Gran Sala) de 21 de diciembre de 2023 (caso *G. K. y otros* y Fiscalía Europea C- 281/22), donde esta reserva de autorización judicial se expande a cualesquiera actuaciones que afectaran a derechos fundamentales.

Ahora bien, ese principio de menor rigor, consecuencia de la menor intensidad de la injerencia, sí afectará al desarrollo jurisprudencial de esta medida de investigación, al menos en dos momentos claramente destacables. Si bien, siguiendo el planteamiento de la sentencia del caso *G. D. y Comissioner An Garda Síochána,* es común a otras modalidades relacionadas con la conservación y tratamiento de datos que la norma nacional que regule el supuesto de la orden de preservación deba garantizar «...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», se permitirá un cierto margen de apreciación a la hora de definir los límites temporales de mantenimiento de la medida, aunque estos hayan de ser por definición perentorios, sujetándolos a la posibilidad de establecimiento de prórrogas justificadas en función de la finalidad perseguida por la medida; y se mostrará igualmente un cierto aperturismo a la hora de definir el alcance de la medida y su no necesaria perfecta sintonía con lo que finalmente hubiera de ser objeto de solicitud de cesión de datos. De hecho, ambas sentencias se muestran abiertas a la posibilidad de que la orden de preservación afectara incluso a personas no sospechosas de haber cometido una infracción criminal, en tanto en cuanto esta delimita-

ción de los datos de tráfico o de localización cuya preservación se ordena se establezca «...sobre la base de elementos objetivos y no discriminatorios, contribuir a la investigación de dicho delito».

2. Especial mención a la exigencia de la gravedad del delito

Las dos sentencias analizadas se muestran especialmente cautelosas con la exigencia de que quede en la norma habilitante claramente delimitada la determinación de los motivos por los que puede acordarse esta retención o preservación rápida; que las infracciones penales para las cuales pueda acordarse esta medida, aparte del interés de la seguridad nacional concernido, tengan naturaleza de graves, y que los datos que se recaben, como corolario del estricto respeto de los principios de proporcionalidad y necesidad, abarquen exclusivamente a datos de tráfico o localización que puedan contribuir a esclarecer los hechos investigados.

Para comprender qué entienden ambas sentencias por delincuencia grave hemos de retrotraernos a la STJUE (Gran Sala) de 2 de octubre de 2018 (caso *Ministerio Fiscal,* asunto 207/16). La sentencia abordaba una cuestión prejudicial planteada por la Audiencia Provincial de Tarragona sobre un supuesto de petición de cesión de datos sobre la asociación del IMEI de un teléfono, objeto de sustracción en un robo violento en el que los autores aparentemente habían empleado una inusitada violencia contra la víctima, con tarjetas SIM que pudieran haberse introducido en el terminal durante un concreto espacio de tiempo.

El TJUE acude a un planeamiento realmente novedoso a la hora de definir ese concepto de delincuencia grave que será esencial a la hora de delimitar el tipo de infracciones criminales que pudieran soportar en términos de proporcionalidad concretas medidas de injerencia afectantes a la confidencialidad de las comunicaciones o la protección de datos de tráfico o localización relacionados con ellas. Se establecería, para ello, un punto álgido del nivel de injerencia, correspondiente a aquellos supuestos en que por la medida o herramienta empleada pudiera obtenerse información detallada sobre datos de la vida privada de las personas afectadas por la medida; y este nivel se reservaría para lo que sería definido como *delincuencia grave*. A partir de aquí se daría forma a una escala decreciente; en la que el grado ínfimo, correspondiente en esencia a lo que en la STJUE del caso *G. D. y Comissioner An Garda Síochána* se definieran como *datos de identidad civil*, se relacionaría con la denominada *delincuencia ordinaria.*

A la hora de definir qué se entendía como delincuencia grave, la sentencia del caso *Ministerio Fiscal* —§§ 102 y 103— decide acudir a la definición que, con carácter ejemplificativo asumiera el precedente de la sentencia del caso *Teles Sverige AB y otros,* que a su vez bebía de la fuente del Preámbulo de la Directiva 2006/24/CE, que, a modo también de ejemplo, citaba al terrorismo y la criminalidad organizada. Pero estaba claro que ello en modo alguno cerraba las puertas a otras posibles modalidades delincuenciales de especial gravedad o trascendencia para el entorno social. Era imposible imaginar que, porque un asesino en serie no perteneciera a una organización criminal o actuara con fines terroristas, no pudiera ser objeto de medidas de investigación tecnológicas.

Por una parte, el propio legislador comunitario garantizaba el empleo de medidas de investigación tecnológica para ámbitos tan concretos como la lucha contra la trata de seres humanos -Directiva 2011/36/UE[21]-, o contra los abusos sexuales y la pornografía infantil[22]. Por otra, no resulta difícil encontrar sentencias del TJUE, que como la STJUE (Gran Sala) de 20 de septiembre de 2022 (casos *V. D.* y *S. R.,* asuntos C-339 y 397/20), abrían las puertas a injerencias de tal naturaleza a otros ámbitos tales como la lucha frente a amenazas contra la integridad de los mercados financieros de la Unión Europea y la confianza del público en los instrumentos financieros[23][24]. Pero era claro que era solo cuestión de tiempo que el TJUE se viera en la tesitura de enfrentarse a nuevos retos en orden a tener que vali-

---

[21] 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.

[22] Directiva 2011/92/UE, del Parlamento Europeo y del Consejo, 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.

[23] En concreto, la 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) núm. 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).

[24] Directiva (UE) 2024/1226 del Parlamento Europeo y del Consejo, de 24 de abril de 2024, relativa a la definición de los delitos y las sanciones por la vulneración de las medidas restrictivas de la Unión, y por la que se modifica la Directiva (UE) 2018/1673, introduce en su art. 13 una nueva categoría de infracciones penales susceptibles de permitir en su investigación el empleo de lo que se definen como *instrumentos de investigación especiales*. Más que consideración de estas infracciones que atentarían contra decisiones adoptadas por la Unión Europea en el contexto de relaciones internacionales como delincuencia grave, el legislador comunitario prefiere hablar de una equiparación o asimilación a este concepto, a

dar nuevos delitos o bienes jurídicos protegidos que pudieran integrar, o al menos asimilarse a él, ese concepto tan abierto como era el de la delincuencia grave. El TJUE no podría aguantar mucho tiempo sin hacer frente a la constante presión de los Estados miembros de la Unión por aclarar o expandir tan estricto concepto de la delincuencia grave; era simplemente una cuestión de tiempo.

La jurisprudencia del TJUE protagonizará un salto realmente espectacular con las SSTJUE de los casos La Quadrature du Net y otros y G. D. y Comissioner An Garda Síochána. Si la primera marcará el sentido de tal evolución, la segunda reforzará lo manifestado por esta, reproduciendo la práctica totalidad de los argumentos jurídicos que sirven de base a tan atrevido salto hacia delante.

La STJUE del caso *La Quadrature du Net y otros* hubo de hacer frente al hábil argumento de la *Cour Constitutionnelle* belga de traer a colación la STEDH, Sección 4.ª, de 2 de diciembre de 2008 (caso *K. U. v. Finlandia,* asunto 2872/02), en la que se imponían severos deberes positivos a los Estados integrantes del Consejo de Europa, en orden a salvaguardar a los menores de los riesgos a los que se somete su indemnidad sexual como consecuencia de su acceso a las redes. Consecuente con tal mandato, el TJUE no solo no pone reparo en asimilar a la delincuencia grave este tipo de atentados, como por otra parte era consecuencia del mandato de la Directiva 2011/92/UE, sino que llega a establecer un criterio de asimilación a tan estricto concepto de delincuencia grave; destacando, además, la existencia de determinados bienes jurídicos prevalentes, entre los que se encontrarían, además, aquellas situaciones en que existiera «... 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».

Acto seguido, cuando ya parecía que el Tribunal había agotado las posibilidades de expansión en la definición del concepto de delincuencia grave, es cuando toma la valiente decisión de reconocer una nueva categoría de valores jurídicos capaces de abrir las puertas a severas medidas de injerencia, en los que se llega a vislumbrar un claro paralelismo con la

---

la hora de abrirse a la posibilidad de adopción de medidas como las que se utilizan «...en la lucha contra la delincuencia organizada o en otros casos de delincuencia grave».

jurisprudencia del TEDH. Hablamos de determinados derechos fundamentales garantidos por la Carta de Derechos Fundamentales de la Unión Europea (CDFUE), a modo de bienes jurídicos protegidos, tales como el derecho a la integridad personal (art. 3), la prohibición de la tortura y tratos inhumanos o degradantes (art. 4), la libertad y seguridad —(art. 6) y, en términos generales, la privacidad (art. 7)[25].

Ahora bien, la misma jurisprudencia se mostró consciente de cómo, con esta expansión de bienes jurídicos que, si bien no eran considerados hasta sus últimas consecuencias delincuencia grave, sí se asimilaban a tales efectos a dicho concepto, se estaba alongando hasta la extenuación este factor determinante del principio de proporcionalidad afectante al interés público en la persecución y represión del delito. Frente a ello, y haciendo uso de una técnica perfectamente parangonable con la conjunción de los arts. 588 bis *a)*.5 y 588 ter.*a)* o 588 septies *a)*.1 LECrim, dibujará en su *§ 50* un esquema de doble control de superación del juicio de proporcionalidad de la primera. El primero, a modo de presupuesto, atendería a la posibilidad de considerar el hecho objeto de investigación como integrable en los tipos penales o bienes jurídicos protegidos considerables delito grave o asimilables a tal concepción. En el segundo nivel de protección, y solo superado el primero, se confrontaría el concreto interés público cuya salvaguardia se pretende con la afectación real de derechos fundamentales de las personas afectadas por la medida. Solamente cuando ese interés público superara al sacrificio impuesto sobre las personas afectadas por la concreta medida, podría considerarse superado el juicio de proporcionalidad.

A estas sentencias han seguido las SSTJUE (Gran Sala) de 30 de abril de 2024 (caso *Giudice delle Indagini Preliminari presso il Tribunale di Bolza-*

[25] «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 art. 15, apartado 1, de la Directiva 2002/58 refleja el hecho de que los derechos consagrados en los arts. 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 art. 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 art. 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 arts. 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—.

no, asunto C-178/22) y (Gran Sala) de 30 de abril de 2024 (caso *La Quadrature du Net y otros,* asunto 470/21). La primera validará finalmente la posibilidad de acudir a un criterio penológico, delitos castigados con una pena privativa de libertad que alcanzaran en su tope punitivo al menos los tres años; pero siempre que la autoridad judicial competente estuviera facultada para denegar una solicitud de injerencia «...habida cuenta de las condiciones sociales en el Estado miembro de que se trate». La segunda llega a dar forma a regímenes de conservación preventiva de datos de asignaciones de IPs de acceso a Internet para la lucha contra delitos en materia de derechos de propiedad intelectual, bajo determinados condicionantes técnicos y de sometimiento, según las circunstancias, a una previa autorización judicial o de autoridad administrativa independiente. Ambas resoluciones fueron publicadas coincidiendo con la finalización del presente trabajo[26].

3. ¿Superatría el art. 588 octies las exigencias de la jurisprudencia del TJUE en cuanto a los principios de primacía y equivalencia del Derecho de la Unión?

La verdad es que la confrontación del art. 588 octies LECrim con los principios de primacía y equivalencia que rigen el ordenamiento jurídico del Derecho de la Unión respecto de las normas nacionales internas coloca en un auténtico compromiso a quien pretenda defender su sintonía. No debe olvidarse que lo que hace el TJUE en las sentencias citadas es dibujar los patrones que han de seguir las normas nacionales internas a la hora de dar contenido normativo a la regulación de las órdenes de preservación referidas a datos de tráfico y localización.

El primer reto resulta difícilmente salvable. No parece precisamente sencillo poder justificar que una orden de preservación rápida case con plazos de conservación que alcanzan a los noventa días, y que pueden duplicarse mediante una prórroga cuya decisión asumiría la misma autoridad policial o fiscal que emitiera la orden. Ambas sentencias hablan de plazos

[26] Realizo un primer acercamiento a la primera de las sentencias en mi trabajo «Hacia una nueva dimensión del principio de proporcionalidad en la injerencia legal sobre comunicaciones en la jurisprudencia del Tribunal de Justicia de la Unión Europea» (*Diario La Ley*, núm. 10538, Sección Doctrina, 3 de julio de 2024, La Ley); y un comentario extenso de la segunda en mi trabajo, pendiente de publicación, igualmente en el *Diario La Ley*: «Conservación generalizada de datos de telecomunicaciones para fines de investigación criminal: nuevos horizontes en la jurisprudencia del TJUE y del TEDH».

perentorios; ajustados a las necesidades a las que atiende la propia naturaleza de este tipo de herramientas de investigación, basadas en la inmediatez temporal de su ratificación o destino a la preparación de la solicitud de autorización por autoridad judicial o administrativa independiente de la orden de cesión de datos relacionada con la orden de preservación. Tres meses es un plazo que a todas luces se muestra excesivo, y más en un contexto en el que la judicialización de la medida depende excesivamente de la presentación de la solicitud u otras formas de puesta en conocimiento de la decisión adoptada. Por mucho que la labor investigadora paralela a la emisión de la orden de preservación puede llegar a provocar que el cometido de seleccionar o identificar los datos cuya cesión ha de interesarse pudiera alongarse razonablemente en el tiempo[27], habría sido más adecuado el establecimiento de plazos mucho más perentorios, prorrogables, incluso por varias veces, basándose en razones suficientemente justificadas. Estamos mucho más cerca de la contrariedad con el Derecho de la Unión que de la posibilidad de conseguir una interpretación conforme con la jurisprudencia del TJUE citada. Lo único que se nos puede ocurrir es una a modo de autorregulación, de drástica reducción, nunca agotamiento, de los generosos plazos marcados por la norma nacional; pero esta solución posiblemente no llegaría a colmar la actitud sin duda exigente del TJUE.

La interpretación que hemos defendido de la aplicación al supuesto de la orden de preservación del mandato del art. 7.1 de la LO 7/2021, en conjunción con las exigencias del TEDH en orden al sentido que ha de darse a esa función de control y supervisión, aún externos, de la autoridad judicial, si permitiría, al menos en mi opinión, una superación de esa exigencia del sometimiento de la medida acordada por autoridad fiscal o administrativa a un control jurisdiccional efectivo; que ya hemos visto que no tiene que ser necesariamente una autorización judicial previa o una confirmación o ratificación de la previa decisión anticipara por razones de urgencia, bastando con una dación de cuenta que permita fiscalizar e incluso dejar sin efecto la medida acordada.

La cuestión sobre el concepto de delincuencia grave precisaría sin duda de una interpretación acomodaticia, en este caso sin duda factible, de la fusión entre los arts. 579.1, 588 ter *a)* y 588 septies *a)*.1 LECrim a esa concepción de origen jurisprudencial. El mimetismo sería pleno en cuanto res-

[27] En el mismo ejemplo antes descrito de la congelación de datos de localización asociados referidos a una concreta estación BTS y a la franja de tiempo en que se supone se ha cometido un asesinato, la labor de identificación de sospechosos sobre los que poder indagar su presencia *electrónica* en ese escenario espacio-temporal podría durar días o semanas.

pecta a la lucha contra el terrorismo y la delincuencia organizada; igualmente, en el supuesto del registro de dispositivos de almacenamiento masivo de datos, podríamos encontrar un cierto grado de identidad con esa asimilación de la protección de la infancia frente a amenazas contra su integridad física y moral, que defendiera la STJUE del caso *La Quadrature du Net y otros,* y la salvaguardia de bienes jurídicos tan trascendentes como son el orden constitucional o la seguridad o defensa nacional, podrían ser fruto muy probablemente de una nueva expansión con tal que se planteara una cuestión prejudicial al respecto. Sin embargo, la opción por la definición del concepto de delito grave en función exclusivamente de la pena impuesta al delito no ha tenido finalmente una acogida expresa en una jurisprudencia del TJUE a la que se planteara, sin éxito, por los representantes de los distintos Estados e instituciones comunitarias personados en las vistas de los correspondientes procedimientos, la necesidad de acudir a tal criterio. Menos la presencia de ese elemento tecnológico de la comisión del delito «... a través de instrumentos informáticos o de cualquier otra tecnología de la información o telecomunicación o servicio de comunicación»; que más tiene que ver más bien con el principio de necesidad de la medida, y que a lo sumo podría servir de criterio adicional en un juicio de proporcionalidad del segundo orden del análisis del supuesto concreto.

Para terminar, y recordando las admoniciones que se hicieran en la STJUE (Sala Sexta) de 17 de noviembre de 2022 (caso *Spetsializiran Nakazatelen SAD,* asunto C-350/21) al caso de la legislación húngara sobre la necesidad de arbitrar vías adecuadas para que los ciudadanos afectados pudieran disponer de *garantías efectivas contra los riesgos de abuso,* la posición de la legislación española debería considerarse ciertamente robusta. El deber de puesta en conocimiento del acto de injerencia adoptado, una vez levantado el carácter secreto de la actuación impuesto por el art. 588 bis *d)*, viene, de hecho, establecido por una norma que, aun ubicada en el contexto de las injerencias sobre comunicaciones, encuentra una indiscutible vocación de expansión a los demás supuestos de investigaciones tecnológicas: El art. 588 ter *i),* además de las normas sobre protección de datos personales que garantizan el derecho de información una vez desaparecido el carácter discreto de la decisión policial o fiscal de preservación de sus datos. Es cierto que la norma precisa de un cierto esfuerzo interpretativo para su conciliación con la jurisprudencia en concreto del TEDH, especialmente en cuanto al diseño de las excepciones a la comunicación personal a todos los afectados ocasionales por el acto de injerencia; pero esa interpretación garantiza un nivel razonable de apertura a vías reaccionales

tanto a las personas directamente afectadas por la medida de preservación, como a desconocidos terceros que se hubieran visto afectados por la decisión como consecuencia de pertenecer sus datos al espectro de información sometida a preservación.