TESIS DOCTORAL

AÑO 2022

VISIÓN POLICIAL DE LA INVALIDACIÓN DE LA DIRECTIVA EUROPEA DE CONSERVACIÓN DE DATOS DE LAS COMUNICACIONES ELECTRÓNICAS. UNA ENCRUCIJADA EN LA LUCHA CONTRA LA DELINCUENCIA GRAVE

LORENZO LUNA ZAMBRANA

PROGRAMA DE DOCTORADO EN UNIÓN EUROPEA

DIRECTOR: DR. D. LUIS MIGUEL GONZÁLEZ DE LA GARZA
PROFESOR DE DERECHO CONSTITUCIONAL DE LA UNED

"Si el hombre fracasa en conciliar la justicia y la libertad, fracasa en todo"

Albert Camus

"Cuando la inocencia de los ciudadanos no está asegurada, tampoco lo está su libertad"

Montesquieu

A mis padres, Antonio y Carmen,
por consagrar su vida a dar a sus hijos una educación

A Marta, por su inquebrantable confianza en mis posibilidades
y por sacrificar muchos momentos de su vida por mis proyectos

A Luis Miguel González de la Garza, mi director de tesis, por su permanente entusiasmo con este proyecto y sus constantes muestras de ánimo y apoyo

SIGLAS Y ABREVIATURAS

APD	Agencia de Protección de Datos
ARCO	Acceso, Rectificación, Cancelación y Oposición
BSI	Basic Subscriber Information, *en inglés*
CATS	Comité de Coordinación en el ámbito de la Cooperación Policial y Judicial en Materia Penal
CdE	Convenio de Europa
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CEDH	Convenio Europeo de Derechos Humanos
CGN	Carrier Grade NAT, *en inglés*
DIM	Detector de identidades múltiples
DOUE	Diario Oficial de la Unión Europea
E2EE	End-to-End encryption, *en inglés*
EC3	European Cybercrime Centre, *en inglés*
ECRIS-TCN	Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países
EJCN	European Judicial Cybercrime Network, *en inglés*
ENISA	European Union Agency for Cybersecurity
EPPO	European Public Prosecutor Office
EURODAC	Sistema europeo de comparación de impresiones dactilares
Europarl	European Parliament, *en inglés*
FRA	Agencia europea para los Derechos Fundamentales
GT29	Grupo de Trabajo del Artículo 29
IA	Inteligencia Artificial
ICQ	Cliente de mensajería instantánea
IMEI	Mobile Equipment Identify, *en inglés*
IMSI	International Mobile Subscriber Identity, *en inglés*
IoT	Internet de las Cosas
IP	Internet Protocol, *en inglés*
JAI	Justicia y Asuntos de Interior
LECRIM	Ley de Enjuiciamiento Criminal
LIBE	Comisión de Libertades Civiles, Justicia y Asuntos de Interior
LSSI	Ley de Servicios de la Sociedad de la Información

OCDE	Organización para la Cooperación y el Desarrollo Económicos
OED	Orden Europea de Detención
OEI	Orden Europea de Investigación
OSINT	Open-Source Intelligence, *en inglés*
OTT	Over-the-top, *en inglés*
PEB	Portal Europeo de Búsquedas
PNR	Passenger Name Record, *en inglés*
PIU	Passenger Information Unit, *en inglés* (UIP, en español)
RCDI	Registro común de datos de identidad
RGPD	Reglamento General de Protección de Datos
SCB	Sistema de correspondencias biométricas
SECA	Sistema Europeo Común de Asilo
SEIAV	Sistema Europeo de Información y Autorización de Viajes
SEPD	Supervisor Europeo de Protección de Datos
SES	Secretaría de Estado de Seguridad
SIM	Subscriber Identity Module, *en inglés*
SIS	Sistema de Información de Schengen
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la UE
STS	Sentencia del Tribunal Supremo
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la información y la comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
TUE	Tratado de la Unión Europea
VIS	Sistema de Información de Visados
VPN	Red privada virtual

INDICE

CAPÍTULO X

INTRODUCCIÓN

Hace menos de un año, ni los más finos analistas podrían haber adivinado que el 24 de febrero de 2022 se daría un giro a la Historia que, incluso a los que tenemos cierta edad, nos parece difícil de creer. Ese día comenzó la invasión rusa a Ucrania, que todavía hoy continúa y no se vislumbra el final, ni cómo será. Lo cierto es que las consecuencias -sin ánimo de establecer una comparación con el sufrimiento que está soportando el pueblo ucraniano- se están sintiendo, con distinta intensidad, en todo el planeta.

Observamos como las fronteras físicas no impiden que los riesgos y amenazas de una situación geopolítica tan inestable como la actual afecte a países situados a muchos kilómetros de distancia del centro de las operaciones; observamos cómo se exige a la comunidad internacional adoptar medidas de forma urgente para ayudar al pueblo invadido; observamos como los líderes políticos mundiales buscan la forma de ayudar a taponar la herida, pero no se ponen de acuerdo sobre la mejor forma de hacerlo, ni del amparo jurídico de las medidas que pretenden adoptar, o del coste económico de su aportación o del tiempo para que su puesta en funcionamiento sea eficaz, entre otras situaciones que a diario oímos, leemos y vemos.

Sirva esta analogía, de triste actualidad, para ilustrar qué queríamos abordar en esta tesis, qué hipótesis de trabajo planteábamos, qué hemos analizado y qué hemos obtenido y propuesto, si es que hemos conseguido nuestro objetivo.

Aunque los ataques terroristas del 11S nos hicieron ver lo frágiles que son nuestras sociedades y que se podía sembrar el terror en nuestras naciones, alejadas de los tradicionales lugares donde librábamos las batallas contra esta lacra; los ciudadanos europeos veíamos a mucha distancia también ese escenario. Sin embargo, en pocos años, en Madrid, en Londres, en Bélgica y otros Estados miembros de la Unión Europea confirmamos que las distancias no estaban tan alejadas para quienes querían cambiar nuestra forma de vida pacífica y en convivencia. Como ante la invasión a Ucrania, los ciudadanos pedían a sus gobernantes que adoptaran medidas para evitar que esto

volviera a ocurrir y para detener y llevar ante los tribunales a quienes habían cometido estas atrocidades.

En el ámbito de la Unión Europea, en las reuniones de urgencia convocadas tras cada uno de los atentados que hemos mencionado, los representantes políticos de los Estados miembros y los responsables de las instituciones europeas mostraban su determinación para desarrollar acciones concretas y daban instrucciones a los técnicos y expertos para que se reunieran y encontraran las mejores herramientas en favor de esos objetivos. Una de estas medidas se materializó en 2005 a través de una propuesta de la Comisión Europea para regular la forma en que se podría utilizar una información muy útil para los proveedores de servicios de telecomunicaciones, que recogían múltiples datos relacionados con las conexiones necesarias para establecer diferentes tipos de comunicaciones entre los individuos; datos que servían a sus fines de negocio y comerciales, pero que podrían tener también utilidad para prevenir amenazas a la seguridad nacional, como las que suponen el terrorismo yihadista, o en la lucha contra la delincuencia. Lo cierto es que los ciudadanos usaban ya en aquel momento cada vez más los teléfonos móviles y Smartphone, y los servicios que se proporcionan a través de Internet se habían extendido a la práctica totalidad de la población.

En 2006, se aprobó una directiva europea que regulaba la forma en la que los proveedores de servicios de telecomunicaciones tendrían que conservar durante un período de tiempo determinado, tanto los datos que servían a sus fines empresariales, como otros que también se podían recoger en las comunicaciones entre personas (datos de tráfico y de localización) y se establecía la obligación de ponerlos a disposición de las autoridades competentes -fundamentalmente las agencias encargadas de la aplicación de la ley- cuando fueran requeridos para ello. Como decíamos, había urgencia para aprobar esta y otras normas, aunque eran conscientes de que el proceso legislativo ordinario de toma de decisiones en la Unión Europea no es demasiado ágil. Los Estados miembros -algunos- habían tomado ya medidas similares en su propio territorio, pero se creía necesario establecer alguna forma de armonización de las medidas nacionales, puesto que se era consciente de que no se podía afrontar desde un punto de vista puramente nacional una amenaza que no entiende de fronteras.

La Directiva en cuestión -Directiva (UE) 2006/24/CE- sufrió el rechazo desde el principio de numerosos actores que de una u otra forma estaban involucrados en el proceso de aprobación o a la hora de ejecutar las medidas que esta recogía. Aun así, se aprobó, entró en vigor y se incorporó al derecho de los Estados miembros tras la transposición a sus normativas nacionales, donde también hubo cierto rechazo y muchas dudas que se llevaron ante el Tribunal de Justicia de la Unión Europea. En 2014, en la sentencia del *caso Digital Rights Ireland y otros*, el Tribunal europeo declaró que la Directiva establecía un régimen de conservación de datos generalizado e indiscriminado que lesionaba gravemente los derechos a la privacidad y a la protección de los datos personales de los ciudadanos, porque adoptaba medidas desproporcionadas. En consecuencia, declaró inválida la Directiva. Una sentencia de 2016, derivada de cuestiones prejudiciales planteadas por Suecia y Reino Unido, determinó que las normativas nacionales aprobadas en transposición de la Directiva anulada no podían aplicarse, por ser contrarias a derecho. No obstante, no todos los tribunales nacionales siguieron la sentencia y no dejaron de aplicar sus normativas nacionales.

En 2017, inmediatamente después de la segunda sentencia, en las instituciones europeas se toma conciencia de la gravedad de la situación y de la necesidad de convocar a los expertos de los Estados miembros y buscar una solución al problema generado. Casi dos lustros después no se han encontrado -o no se han querido encontrar- las claves para resolver la ecuación. Nosotros, que asistimos de forma directa a esos momentos iniciales -desde el Consejo de la Unión Europea- en los que se decidió analizar la situación y ofrecer respuestas, observamos ya desde el principio que no sería fácil. El tiempo nos ha dado la razón. En consecuencia, nos planteamos desarrollar una investigación con el objetivo de buscar la mejor forma de acometer el problema y encontrar las piezas de un *puzle* complicado, las claves que sirvan para decidir si este debe ser afrontado de forma independiente por cada Estado miembro -como se había hecho hasta ese momento- o a través de una solución europea -como la que fijó la Directiva invalidada- y, al mismo tiempo, delimitar un marco previo para establecer un nuevo régimen de conservación de datos de las comunicaciones electrónicas con aquellos aspectos fundamentales que permitan cumplir con los requerimientos del Tribunal, respetando los derechos y libertades fundamentales de los ciudadanos, pero garantizando también que los datos sirvan eficazmente a los fines para los que se había

aprobado la Directiva de 2006. Efectivamente, una ecuación cuya resolución podría permitir salir de la encrucijada en la que se encuentra -desde hace ya demasiado tiempo- la investigación penal de determinados delitos graves que se sirven de los metadatos (datos de tráfico y localización; distintos del contenido) de las comunicaciones electrónicas.

A lo largo del tiempo que nos ha ocupado el estudio, hemos observado que la bibliografía y otros documentos que abordan la materia, lo hacen casi exclusivamente desde el punto de vista de la injerencia en los derechos fundamentales de los ciudadanos de las medidas que previó la Directiva de 2006. Sin embargo, no se ha analizado la otra cara de la moneda: los efectos de esas medidas en la lucha contra la delincuencia grave y las consecuencias de la invalidación de la norma. Partimos de la premisa de que, para adoptar medidas proporcionadas, deben ponderarse adecuadamente los intereses en juego y alcanzar un adecuado equilibrio, y ello requiere conocer también las dificultades y las posibilidades para establecer un nuevo sistema de conservación de datos de las comunicaciones electrónicas. Para ello, creemos que es fundamental también aportar la visión de quienes están llamados a garantizar la seguridad de los ciudadanos y profundizar en la complejidad del sistema de toma de decisiones en un ámbito político tan particular como es la Unión Europea.

A tal fin, hemos abordado diferentes materias, unas antiguas, sobre las que hay mucha documentación y doctrina; otras muy novedosas, sobre las que apenas hay estudios relevantes; y otras de características muy técnicas, que se alejan de nuestro objetivo. Esta última categoría (el ámbito técnico y tecnológico) no será analizada en profundidad, por cuanto la tesis está enmarcada en mayor medida en un ámbito jurídico y de procedimiento de toma de decisiones institucionales, y no en el cuestionamiento de los conceptos técnicos que rodean al sector de las telecomunicaciones. Para ello, nos hemos servido de una combinación de fuentes legislativas, del análisis jurisprudencial pertinente a nuestra materia y de la producción científica y doctrinal existente; complementada con la documentación disponible de las principales instituciones europeas (Consejo de la Unión Europea y Comisión y Parlamento europeos, y otras agencias y organismos consultivos) y la experiencia propia en el trabajo en algunas de

esas instituciones y en el ámbito policial a nivel nacional e internacional. Hemos aplicado el método científico deductivo, que nos permitirá llegar a aspectos concretos y específicos del problema y aportar claves para su resolución.

Reseñaremos a continuación un sumario de aquello que nos ha servido de guía en la investigación hacia la redacción de unas propuestas concretas que esperamos que contribuyan a un final aceptado por la mayoría de las partes, si no todas.

Aunque la Directiva 2006/24/CE era una norma europea relativamente reciente, como relatábamos, en los primeros años de vida fue ya estudiada por numerosos autores, poniendo de manifiesto fundamentalmente -la gran mayoría de ellos- los problemas que generó antes de su concepción y la injerencia en los derechos fundamentales de los ciudadanos, obviando el análisis respecto de su contribución a la lucha contra el delito y en qué medida contribuía a mejorar la seguridad de los ciudadanos. Sin embargo, puesto que su invalidación se produjo en 2014 y, todavía hace poco más de un mes, (finales de septiembre) el Tribunal de Justicia de la Unión Europea se ha pronunciado nuevamente al respecto, no ha habido tiempo material para que los expertos aborden en profundidad las implicaciones de estas sucesivas sentencias ni la forma de abordar un nuevo sistema de conservación. Por tanto, creemos que el objeto de esta tesis es actual, pertinente y novedoso.

El **primer capítulo** acomete el recurrente e irresoluble dilema que enfrenta a la Seguridad y la Libertad y analiza las claves de esa relación, que surge cada vez que se produce un hecho desgraciado -como los atentados que hemos citado- y confronta las posiciones de quienes defienden que se aprovechan estas situaciones para dar más poder a las agencias encargadas de la aplicación de la ley y se restringe la libertad de los ciudadanos; y de quienes consideran que la Seguridad es un derecho que también ha de ser garantizado y protegido y, para ello, se ha de dotar de herramientas adecuadas a los servidores públicos que tienen encomendada la misión de velar por las personas.

En el **segundo capítulo** se analizan dos de los derechos fundamentales que se ven afectados por las medidas de conservación de datos que preveía la Directiva de 2006: el derecho a la privacidad y el derecho a la protección de los datos de carácter personal; su nacimiento y evolución, principalmente en la Unión Europea, y su tratamiento en el ámbito de la policía y la justicia penal, con la idea de entender en qué medida se puede producir una injerencia desproporcionada que lleve a la invalidación de una norma europea aprobada en el marco de las competencias legislativas de las instituciones de la Unión.

El **capítulo tercero** centra la atención en escrutar si los datos de tráfico y de localización que se generan en las comunicaciones electrónicas -el continente de una comunicación, por contraposición al contenido en sí mismo- son realmente tan importantes como consideran los servicios policiales a los efectos de la aplicación de la ley y en qué medida contribuyen a la investigación penal. Se analiza también qué acciones podrían aplicarse para que esta información pudiera seguir siendo útil a los efectos que preveía la Directiva invalidada y, al mismo tiempo, se respetaran los derechos y libertades fundamentales de los ciudadanos europeos.

En el **capítulo cuarto** estudiamos el papel que desarrolla el Tribunal de Justicia de la Unión Europea en la defensa de los derechos fundamentales de los ciudadanos y su evolución desde los comienzos hasta ahora, hasta el punto de que, para algunos autores, se ha convertido en un *Tribunal Constitucional europeo*, incluso difiriendo del criterio del Tribunal Europeo de Derechos Humanos. Consideramos fundamental comprender esta evolución para entender en qué medida su doctrina puede afectar a los Estados miembros y condicionar el margen de actuación de los tribunales nacionales, e incluso de los legisladores nacionales, respecto de materias que no están *comunitarizadas*.

El **quinto capítulo** versa sobre los requisitos para justificar la injerencia en los derechos fundamentales, en la idea de que ningún derecho es ilimitado. Teniendo en cuenta que la invalidación de la Directiva de 2006 fue debida a que establecía medidas

que provocaban una injerencia desproporcionada en determinados derechos, consideramos fundamental estudiar los elementos que conforman este principio, como también el de necesidad, y tratar de encontrar pautas o guías que permitan ponderar y equilibrar la colisión entre derechos, en general, y respecto de los derechos afectados por las medidas de conservación de datos de las comunicaciones electrónicas, en particular.

El **capítulo sexto** se convierte en uno de los centrales y, en consecuencia, más extensos, pues analizamos las distintas sentencias del Tribunal de Justicia, desde el *Caso Digital Rights Ireland* hasta hoy, a través de las que se ha sentado una doctrina que nos obliga a la hora de buscar soluciones y hacer propuestas para un nuevo sistema de conservación de datos. Observaremos que, si bien se mantiene la postura general inicial, se han ido modulando determinados aspectos, que hemos analizado en profundidad, que ofrecen claves importantes -unas positivas y otras menos favorables- en cuanto a su contribución o no a una solución de consenso entre los Estados miembros y entre las instituciones europeas con responsabilidad en el proceso legislativo. Analizamos también la reacción que este nuevo escenario ha producido en los Estados miembros, a nivel judicial y policial.

El **séptimo capítulo** pretende comparar el sistema de conservación de datos invalidado con otras bases y sistemas de datos importantes y recientes en la Unión Europea, que sirven igualmente a fines de prevención y persecución de la delincuencia y que se basan también en la recogida y almacenamiento de datos que son puestos a disposición de las autoridades competentes y tratados con fines policiales y judiciales. Hablamos del sistema PNR *(Passenger Name Records, por sus siglas en inglés)* y de la *Interoperabilidad* de determinadas bases y sistemas europeos. Se describirá la arquitectura general de cada uno de ellos, su concepción y funcionamiento, para poder extraer conclusiones sobre las diferencias y similitudes y buscar alguna clave que ayude al nuevo enfoque de la conservación de datos de las comunicaciones electrónicas.

El **capítulo octavo** identifica y profundiza en el cambio de paradigma introducido por el Tribunal y analiza cómo se abordó la nueva situación en Bruselas y cómo se materializa la toma de decisiones en la Unión Europea y el procedimiento legislativo que se sigue a la hora de aprobar normas como la que se invalidó en 2006; o como la que habría que aprobar en el futuro, si la Comisión presentara una nueva propuesta. Se estudian también las relaciones entre las instituciones europeas y las dificultades en la negociación de los expedientes legislativos, de tal forma que en ocasiones pueden *dejarse morir* sin acuerdo o se alcanza un acuerdo que no mejora la situación anterior; todo ello con consecuencias evidentes en los derechos de los ciudadanos y en términos de credibilidad de la Unión Europea en su conjunto.

El **capítulo noveno** presenta nuestras propuestas, el resultado de nuestra investigación, en forma de ideas generales y claves de *lege ferenda* que deberían tener en cuenta los decisores de la Comisión a la hora de presentar una nueva propuesta de Directiva europea de conservación, así como otros elementos que deberían quedar al margen -para ser sustanciados mediante una norma distinta- o recogidos solo a modo de indicación. También se incluyen consideraciones generales y particulares que consideramos que deberían guiar las negociaciones entre el Consejo y el Parlamento, para conseguir una norma respetuosa con los derechos fundamentales de los ciudadanos, pero igualmente eficaz en la lucha contra la delincuencia grave -dejamos fuera de la propuesta la conservación de datos con fines de prevención de amenazas a la seguridad nacional-, por los motivos que se exponen en el capítulo.

Por último, cierra la tesis el **capítulo décimo**, correspondiente a las conclusiones, en la que la principal es la primera -que aquí esbozamos: la clave del éxito está en la *voluntad y la determinación* para asumir la nueva realidad y vencer la resistencia al cambio, siendo conscientes de que el nuevo sistema de conservación de datos de las comunicaciones electrónicas no volverá a ser como el anterior, y asumiendo que es perentorio buscar alternativas en el marco de la nueva realidad, en beneficio de los ciudadanos y de su seguridad, con respeto de sus derechos y libertades fundamentales. Para ello, esperamos que esta tesis pueda servir en alguna medida; al menos, ese ha sido el propósito que nos ha guiado.

CAPÍTULO I. EL DILEMA LIBERTAD VS. SEGURIDAD

No parece estar en cuestión, al menos de forma generalizada, que la seguridad es clave para el desarrollo de una sociedad democrática. Hay dos vertientes extendidas y contrapuestas de la relación entre ambos conceptos: una, que considera que a mayor seguridad se produce una mayor garantía del ejercicio de los derechos; otra, que defiende que a mayor seguridad se disfruta de menor libertad. Aunque no queremos referirnos al ámbito nacional, sí se mencionarán en ocasiones conceptos de la legislación española que puedan ilustrar de forma clara lo que queremos expresar. En ese sentido, como indica Brandariz García (2014; 315)[1], el art. 17.1 de la Constitución Española plasma el entendimiento de la Seguridad y la Libertad como conceptos sinérgicos, aunque él considera su relación tendencialmente contradictoria.

De lo que no cabe duda es que solo en un contexto de razonable seguridad puede disfrutarse de los derechos fundamentales[2]. Pérez Royo (2010; 7)[3] señala que entre Libertad y Seguridad no hay tensión, porque la segunda forma parte de la primera. A mayor abundamiento, actualmente se reconoce que la seguridad puede limitar otros derechos de forma legítima, en contraposición a visiones anteriores en las que se defendía que los derechos eran absolutos y no podían ser limitados. Son abundantes los ejemplos que ilustran esa limitación, pero nos ceñiremos más adelante a algunos concretos a los efectos de nuestra tesis.

Fuere como fuere, en los últimos años las cuestiones de seguridad siempre han emergido como elementos para justificar tales limitaciones, pero de forma particular, en las últimas décadas, propiciado por una serie de riesgos y amenazas emergentes, se ha intensificado la relevancia de la Seguridad y este concepto se ha convertido en un elemento constante en las discusiones políticas y sociales a nivel mundial; sin excluir al

[1] BRANDARIZ GARCÍA, J.A. *"¿Una teleología de la seguridad sin libertad? La difusión de lógicas actuariales y gerenciales en las políticas punitivas"*, en Fundamentos nº 8, La Metamorfosis del Estado y del Derecho, 2014 pp. 313- 354, p. 315, en https://www.unioviedo.es/constitucional/fundamentos/octavo/pdfs/Brandariz-Teleologia.pdf

[2] Esta relación es compleja y presenta múltiples aristas y aspectos controvertidos. En este capítulo se analizarán esas características, con la intención de alcanzar un consenso al menos sobre la necesidad de buscar un equilibrio entre ambas, que permita compadecer las dos vertientes presentadas: positiva y negativa.

[3] PEREZ ROYO, J. *"La democracia frente al terrorismo global"*, en Terrorismo, democracia y seguridad, en perspectiva constitucional, Barcelona, 2010, pp. 7-12, p.7.

ámbito de la Unión Europea -ámbito que nos interesa más. Serra Cristóbal (2016; 488)[4] cree que bajo pretextos de seguridad nacional se han defendido argumentos para la adopción de medidas que parecen más bien encaminadas a la limitación de la Libertad y no tanto a garantizarla y se muestra a favor de la existencia [en la Unión Europea] de instrumentos y principios que forman parte de los fundamentos propios de esta organización política, que pueden ayudar en la adopción de políticas de lucha contra el terrorismo [y contra la delincuencia grave] que no supongan un sacrificio excesivo o desproporcionado de las libertades de los ciudadanos.

Rodotà (2006; 58)[5] no niega la necesidad de adoptar medidas para luchar contra el terrorismo [entendemos que también estaría de acuerdo en la adopción de medidas contra el delito grave o la criminalidad organizada, aunque son fenómenos con características diferentes, pero en muchos casos relacionados] y apoya el aprovechamiento de las oportunidades que ofrecen las tecnologías electrónicas para ese fin. No obstante, considera que en sociedades democráticas no puede obviarse la necesidad de confrontar las necesidades en materia de seguridad con los derechos fundamentales de los ciudadanos; argumento con el que estamos plenamente de acuerdo, entendiendo que confrontar implica ponderar ambas partes y buscar un adecuado equilibrio. Castellanos Claramunt (2022; 109)[6], en un análisis sobre transparencia y participación ciudadana, al referirse a la capacidad de adaptación de la democracia, sostiene que *"por muchos que sean los problemas aparejados a ella, el sentimiento de proteger un sistema basado en la libertad y en la participación de los ciudadanos en los asuntos públicos pervive pese a las diversas coyunturas"*. Sin duda, no podemos entender en momentos actuales y en un entorno europeo que no se otorgue participación a los ciudadanos en el proceso de adopción de medidas y de implementación de políticas que afectarán de forma directa a sus derechos y libertades. De esa forma, consideramos que podrá conseguirse en mayor medida el sentimiento de

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

[5] RODOTÀ, S., *"La conservación de los datos de tráfico en las comunicaciones electrónicas"*, en Segundo Congreso sobre Internet, derecho y política: análisis y prospectiva, pp. 53-60 http://www.uoc.edu/idp/3/dt/esp/rodota.pdf

[6] CASTELLANOS CLARAMUNT, J., *"Transparencia y participación ciudadana: la lucha contra la corrupción como eje vertebrador del proceso democrático"*, Revista Española de la Transparencia, nº 15, 2022, pp. 107-129, p. 109.

apropiación o aceptación. Entendemos que el fracaso de las medidas que preveía la directiva que nos proponemos estudiar tuvo en parte que ver con ese déficit de participación.

Sin ser exhaustivos, podemos citar el terrorismo internacional, la aparición de nuevos Estados fallidos, las potenciales armas de destrucción masiva o el reciente resurgimiento de las armas nucleares; o la lucha por los recursos energéticos o los movimientos migratorios derivados de situaciones de guerra, inestabilidad política o pobreza extrema, como algunos de los riesgos emergentes o amenazas que en los últimos tiempos han aparecido o vuelto, por desgracia, a las agendas nacionales [pensemos en la invasión rusa de Ucrania y cómo los elementos citados se han puesto de manifiesto]. La mayoría de los países tienen en cuenta estos riesgos a la hora de diseñar sus políticas y estrategias de seguridad nacional, y de ofrecer opciones de respuesta, pero sin que sean desproporcionadas en su afectación o injerencia en otros derechos. A este respecto, afirma López Aguilar (2017; 580)[7] que en un momento de la historia como el actual, *"la securitización"* ha emergido como no lo había hecho antes como prioridad política y ha impactado de forma notable en el frágil equilibrio entre Libertad y Seguridad.

Encontrar un equilibrio que satisfaga a la sociedad, respecto de este dilema *"Libertad vs. Seguridad"*, surge de forma reiterada en función de acontecimientos concretos que llevan a los decisores políticos a adoptar medidas de acción contra algún riesgo o amenaza concretos a la libre convivencia de sus ciudadanos. Dependiendo del momento que se considere, las posiciones mayoritarias tienden hacia un lado u otro, pero parecen inclinarse habitualmente hacia el pensamiento de que la Seguridad ha sido preponderante por encima de la Libertad[8].

[7] LÓPEZ AGUILAR, J.F., *"La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EE. UU*"., en UNED. Teoría y Realidad Constitucional, núm. 39, 2017, pp. 557-581, p. 580.

[8] El primer y más clásico pensamiento que nos viene a la cabeza es el de las reacciones a los atentados del 11-S en los Estados Unidos, pero hay otros acaecidos en suelo europeo que servirán de ejemplo para la adopción de medidas que analizaremos más adelante.

El reto que se ha presentado siempre y que nos toca también acometer ahora es el de buscar un equilibrio aceptable entre estos dos conceptos, que garantice el libre ejercicio de los derechos fundamentales y de las libertades públicas, que constituyen los verdaderos elementos sobre los que se construyen nuestras democracias y el modelo de sociedad de convivencia pacífica.

1. Un debate recurrente

Son muchas las ocasiones en las que comenzamos un análisis sobre la adopción de medidas que comprendemos que son necesarias para garantizar la seguridad de nuestros ciudadanos, que parten de los atentados del 11 de septiembre de 2001 (11-S) en los Estados Unidos de América (EE. UU), a los que se unen otros que, por desgracia, han ocurrido en años sucesivos, cometidos por parte de redes de terrorismo islamista yihadista. Es el propio ciudadano quien exige a sus gobiernos la adopción de políticas hacia un mayor grado de seguridad. En consecuencia, de forma recurrente, surge el debate entre la relación Seguridad/Libertad y la afectación a los derechos individuales y colectivos de los ciudadanos. Sin embargo, no es un debate nuevo, ni nunca se han vislumbrado posiciones claras en un sentido u otro. Entendemos que quizás esta falta de posición nítida es lo que hace que sea un debate abierto e inconcluso y que se retome constantemente ante hechos concretos, de una forma que coloquialmente se denomina *"en caliente"*, abandonándose cuando la situación se enfría, a la espera del siguiente suceso y reacción posterior en el mismo sentido, convirtiéndose en una especie de círculo vicioso. Más bien, de acuerdo con Marsal Muntalá (2005; 220)[9], *"es un debate que hunde sus raíces en la historia de la sociedad y el pensamiento y especialmente desde que se han ido sentando las bases de las sociedades democráticas*", por lo que podemos asumir que se trata de una característica propia del pensamiento crítico que se ha visto intensificada a medida que se consolidaba la democracia en los diferentes países; desde luego, en otros países concretos que todos podemos imaginar y podríamos enumerar, se justician las reticencias que gran parte de la doctrina muestran en este debate, por cuanto, la Seguridad está muy por encima de otros derechos de los ciudadanos en esos países.

[9] MARSAL MUNTALÁ, J., *"Seguridad versus Libertad",* Arbor, 2005, pp. 219-226, p. 220, en http://arbor.revistas.csic.es

Los ámbitos en los que se plantea este debate son muy variados: seguridad en el trabajo, seguridad frente a desastres naturales; frente a riesgos químicos, u otros riesgos internos o externos; etcétera. Y, cómo no, también en el de la seguridad nacional, pública y ciudadana. En unos u otros casos, como decíamos, en momentos de amenazas concretas o de cambios sociales profundos, los ciudadanos incrementan el nivel de exigencia. Por ello, a principios de siglo, con los atentados del 11-S, se dan de forma conjunta esas circunstancias y, en consecuencia, se acentúan también las exigencias de los ciudadanos. Cosa distinta es cómo responden las autoridades y si las medidas que adoptan satisfacen o no las expectativas de los ciudadanos.

Al mismo tiempo, y de forma indisoluble, la Libertad se configura como otro de los valores de nuestras democracias y, en ese sentido, también surgen exigencias ciudadanas para que su ejercicio sea efectivo y pleno. Otro elemento fundamental en este entorno es el establecimiento de controles para hacer frente a aquellas circunstancias que puedan amenazar nuestros derechos y libertades y su ejercicio en una sociedad democrática.

De forma concreta, el ejercicio de las libertades se ha ido concretando a lo largo del tiempo en una serie de derechos particulares: a la intimidad, al libre movimiento, a la libertad de reunión, etcétera. La máxima expresión de estas ha dado lugar a los llamados derechos humanos y fundamentales.

Según se consulte a unos u otros, es habitual [casis tradicional] que se defiendan teorías que ponen un mayor o menor énfasis en la Seguridad o en la Libertad y el respeto de los derechos ciudadanos. Pero sí hay un cierto consenso en que ambos están ligados y, de esa forma, como indicábamos antes, no puede ejercerse la libertad sin unas ciertas condiciones -mínimas- de seguridad. Las prácticas de convivencia se han ido ajustando a lo largo de la historia, pero manteniendo siempre ese pulso vivo e inconformista de cada una de las partes. De hecho, las medidas adoptadas hacia un lado u otro muestran una difícil coexistencia. Ejemplos de ambas partes podemos encontrar sin demasiado esfuerzo tanto en los Estados Unidos como en Europa. Adelantándonos a

capítulos siguientes, es ilustrativo de lo que venimos indicando, lo que asevera Rebollo Delgado (2008; 14 y ss.)[10], al comparar la regulación en materia de vida privada y protección de datos en Europa y Estados Unidos; observa similitudes, pero también una diferencia fundamental y pertinente para el problema que estamos analizando:

> *"… aunque entre ambos [Europa y Estados Unidos] subyace una diferencia muy significativa, y que irradia a todos los ámbitos (normativo, institucional, doctrinal y jurisprudencial). Radica ésta en relación o ponderación de estos derechos con otro de los ejes de ambos ordenamientos jurídicos, y que es la seguridad. En Estados Unidos presenta menos problema esta relación, o la interpretación se suele decantar en beneficio de la seguridad".*

Más adelante entraremos de lleno en las medidas que motivan esta investigación. No obstante, en esto como en muchas otras facetas de la vida, como indica Marsal Muntalá (2005; 221)[11]: *"el análisis y valoración que podamos hacer de ellos dependen también en gran manera de nuestras visiones del mundo y nuestras posiciones políticas"*. Dejaremos al margen ambas en este documento, de forma que lo que aquí se exponga y argumente sea desde el análisis y rigor científico.

La actual Unión Europea comenzó a formar un espacio político, en el que viven ahora más de quinientos millones de personas, con el establecimiento de un mercado único, que con el Tratado de Maastricht de 1992 pasa a configurarse también como un espacio de libertad de movimiento y de circulación mediante un espacio legal armonizado. En ese tiempo, aparecen derechos que son considerados como comunitarios y, entre otros, dan lugar a la creación del Espacio de Libertad, Seguridad y Justicia (ELSJ) que se desarrolla posteriormente en el programa de Tampere (1999-2004) y de la Haya (2004-2009). Sitúa Tomás Mallén (2014; 218)[12] en ese momento la irrupción de la *"problemática conciliación entre libertad y seguridad en el Derecho primario u originario"*. Ya desde entonces se busca equilibrar el respeto de

[10] REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea*, Dykinson, Madrid, 2008, p. 14 y ss.

[11] MARSAL MUNTALÁ, J., *"Seguridad versus Libertad…", op. cit*., p. 221.

[12] TOMÁS MALLÉN, B., *"Privacidad versus seguridad en el ámbito europeo"*, en Fayos Gardó, A. y Conde Colmenero, P., *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2014, pp. 215-241, p. 218.

determinados derechos fundamentales con la seguridad respecto del intercambio de información y, de forma particular, en el respeto a la privacidad y a la protección de los datos de carácter personal. De hecho, en la Comunicación de la Comisión al Parlamento Europeo y al Consejo en el que se detallaban las diez prioridades del Programa de La Haya, se hace referencia a que el intercambio de información no es admisible ilimitadamente, sino en el marco de un equilibrio adecuado entre seguridad y vida privada, respetando plenamente los derechos fundamentales a la intimidad y a la protección de datos, así como el principio de disponibilidad de la información[13].

Posteriormente, ya en los años 2010 a 2014, el Programa de Estocolmo establece las prioridades de la UE respecto al ELSJ durante ese marco temporal, a partir de los logros de los anteriores programas y mirando al futuro de la Unión y del devenir de sus ciudadanos[14], con el reto de asegurar el respeto y la integridad de las libertades fundamentales, garantizando al mismo tiempo la seguridad en Europa. Para ello, se propone también mejorar la protección de los datos personales, como un derecho más de los ciudadanos europeos de acuerdo con la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE)[15], y en particular los artículos 7 y 8 de esta; derechos que ahora, con el Tratado de Lisboa[16] en vigor, tienen el mismo valor jurídico que los Tratados y, en consecuencia, obliga también a los Estados miembros de la Unión. No obstante, respecto del derecho a la protección de los datos personales y a la privacidad, sigue estando en manos de los Estados miembros la posibilidad de adoptar medidas y e iniciativas en materia de seguridad nacional, lo que no permite desplegar en toda su plenitud la protección de esos derechos fundamentales. Además, según el artículo 276

[13] Vid. Comunicación de la Comisión al Consejo y al Parlamento Europeo, Programa de La Haya: diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia, Bruselas, 10.5.2005, *COM (2005) 184 final*, en http://www.eur-lex.europa.eu/ES/legal-content/summary/the-hague-programme-10-priorities-for-the-next-five-years-html, consultado el 12 de julio de 2022.

[14] Vid. Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano, aprobado por *el Consejo de Justicia y Asuntos de Interior el* 1 de diciembre de 2009, en https://eur-lex.europa.eu/ES/legal-content/summary/the-stockhom-programme.html

[15] La Carta de los Derechos Fundamentales de la Unión Europea fue aprobada en 2010 y publicada en el DOUE de 30 de marzo de ese año. Para profundizar, vid. https://www.boe.es/doue/2010/083/Z00389-00403.pdf

[16] Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea (2007/C 306/01), publicado el 17 de diciembre de 2007, en https://www.boe.es/doue/2007/306/Z00001-00271.pdf

del Tratado de Funcionamiento de la Unión Europea (TFUE)[17], el Tribunal de Justicia de la Unión Europea (TJUE) no es competente para enjuiciar la proporcionalidad de las medidas adoptadas por los Estados miembros relacionadas con el orden público y la Seguridad Interior. En consecuencia, el control de legalidad y, por añadidura, de proporcionalidad de las medidas, deberá ser ejercido por los tribunales nacionales (Alonso, 2010; 8)[18]. Más adelante veremos que esta afirmación ha quedado matizada posteriormente por la jurisprudencia comunitaria. Aunque no hubiera sido así, como es evidente, esa supuesta falta de competencia no es óbice para que, sean las políticas que sean, respeten estas la dignidad humana, la libertad, los derechos de las personas, etcétera, según reza el artículo 2 del TFUE[19].

A mayor abundamiento, el Tratado de Lisboa también prevé que los Estados miembros se encuentren en el Consejo de la Unión Europea para fomentar e intensificar la cooperación en materia de Seguridad Interior[20]. Vemos que prevé reunir a los Estados miembros para llevar a cabo esas acciones, no pudiendo actuar la Unión de forma autónoma o independiente. Bien es cierto, más en los tiempos que corren, que los Estados miembros no pueden afrontar de manera independiente los retos a la seguridad a los que todos nos enfrentamos, lo que sirve a la Unión como justificación para proponer e iniciar acciones que después los Estados miembros, junto con el Parlamento, transforman en actos legislativos; bajo el argumento de que una acción coordinada de

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

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

[19] Artículo 2 del TFUE: *"La Unión se fundamenta en los valores de respeto de la dignidad humana, libertar, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Estos valores son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres"*.

[20] Artículo 71 del TFUE: *"se creará un comité permanente en el Consejo con objeto de garantizar dentro de la Unión el fomento y la intensificación de la cooperación operativa en materia de seguridad interior. Sin perjuicio del artículo 240, dicho comité propiciará la coordinación de la actuación de las autoridades competentes de los Estados miembros. Podrán participar en sus trabajos los representantes de los órganos y organismos de la Unión afectados. Se mantendrá informados de dichos trabajos al Parlamento Europeo y a los Parlamentos nacionales"*.

todos será más eficaz ante las amenazas transnacionales. Aun así, siempre será sin perjuicio de las responsabilidades nacionales en materia de orden público y Seguridad Interior[21]. Este mecanismo de cooperación reforzada podría darnos alguna pista o alternativa de solución al problema que vamos a analizar y que valoraremos al final de nuestra investigación.

El concepto de *"Seguridad Interior"* es muy amplio y seguramente diferente en alcance y en matices para cada uno de los países a los que interroguemos. Esto, como en otros ámbitos, implica que la interpretación que cada país haga del concepto impactará sobre los ciudadanos de una forma distinta, con mayor o menor intensidad, y algunos de sus derechos y libertades podrán sufrir limitaciones también de forma diferente. Nos referimos de forma particular a la privacidad y a la protección de los datos personales. El propio Tratado de la Unión Europea (TUE)[22], en su artículo 4.2 nos da alguna referencia sobre qué podemos entender o interpretar como incorporado en ese concepto; al menos, delimita qué competencias quedan excluidas o no atribuidas a la Unión y qué tiene que ver con la Seguridad Interior:

> *"La Unión respetará la igualdad de los Estados miembros ante los Tratados, así como su identidad nacional, inherente a las estructuras fundamentales políticas y constitucionales de éstos, también en lo referente a la autonomía local y regional. Respetará las funciones esenciales del Estado, especialmente las que tiene por objeto garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional. En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro".*

Es oportuno y necesario citar aquí este artículo y especialmente las funciones de los Estados en cuanto a garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional, por cuanto serán conceptos relevantes que

[21] Artículo 72 del TFUE: *"el presente título se entenderá sin perjuicio del ejercicio de las responsabilidades que incumben a los Estados miembros en cuanto al mantenimiento del orden público y la salvaguardia de la seguridad interior".*

[22] Tratado de la Unión Europea, de 7 de febrero de 1992, firmado en Maastricht (conocido por ese nombre, al que ya nos hemos referido en párrafos precedentes a esa nota), publicado en el DOUEC núm. 340, de 10 de noviembre de 1997, vigente desde el 1 de mayo de 1999 y revisión vigente desde el 1 de septiembre de 2016, en https://noticias.juridicas.com/base_datos/Admin/tue.html

manejaremos más adelante en el análisis de las sentencias del TJUE sobre la Directiva europea de Conservación de Datos de 2006[23]. *Esta Directiva constituye el punto de partida al establecimiento de un sistema a nivel europeo de conservación de datos de las comunicaciones electrónicas (al margen de la comunicación en sí misma), del que se derivaron regímenes nacionales armonizados, y que se ha desmoronado posteriormente, creando una situación que nos proponemos estudiar. Por tanto, es el elemento material central para nuestra tesis.*

Una parte de los expertos considera que el uso de esta *"cláusula habilitante"* sirve a los Estados miembros para justificar que cualquier acción en materia de seguridad debe excluir a la Unión de forma unilateral, por ser un coto reservado exclusivamente a los Estados miembros. Según Rizzo (2019; 148)[24]: *"no sólo para el ELSJ, sino en referencia a todo el Tratado".* Para Serra Cristóbal (2016; 490)[25], el Tratado de Lisboa incluso ha reforzado esta prerrogativa nacional. Sin embargo, no debemos olvidar, como hemos indicado antes, que hoy todos los países sujetos a reglas democráticas *están obligados*[26] a poner en común medidas compartidas ante retos comunes y, en eso, la Unión Europea, aunque no sea por la vía de la *imposición de una competencia*, está llamada a colaborar y a aportar soluciones. Lógicamente, cada Estado miembro intentará ceder lo menos posible de su soberanía y pedir -en ocasiones exigir, que lo hagan los demás. Es el *juego* de las largas negociaciones en el ámbito de las instituciones europeas[27]. Para ello, como recoge el artículo 83 del TFUE:

> *"El Parlamento Europeo y el Consejo podrán establecer, mediante directiva adoptada con arreglo al procedimiento legislativo ordinario, normas mínimas relativas a la definición de las infracciones penales y de las sanciones en ámbitos delictivos que sean de especial gravedad y tengan una dimensión*

[23] Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, en https://www.boe.es/doue/2006/105/L00054-00063.pdf.

[24] RIZZO, G., *Derecho a la privacidad y seguridad en el espacio público europeo*, tesis doctoral, Universidad Carlos III de Madrid, 2019, recuperado en Derecho a la privacidad y seguridad en el espacio público europeo (uc3m.es), p. 148.

[25] SERRA CRISTÓBAL, R., *"Los derechos fundamentales en la encrucijada…", op. cit.*, p. 490

[26] Entiéndase la obligación no desde el punto de vista legal, sino moral y de eficiencia en la consecución de los fines propuestos.

[27] En un capítulo aparte analizaremos la dinámica de uno de los procedimientos legislativos más usados actualmente en la Unión Europea, que introdujo el Tratado de Lisboa: el procedimiento ordinario, anteriormente llamado de codecisión.

transfronteriza derivada del carácter o de las repercusiones de dichas infracciones o de una necesidad particular de combatirlas según criterios comunes. Estos ámbitos delictivos son los siguientes: el terrorismo, la trata de seres humanos y la explotación sexual de mujeres y niños, el tráfico ilícito de drogas, el tráfico ilícito de armas, el blanqueo de capitales, la corrupción, la falsificación de medios de pago, la delincuencia informática y la delincuencia organizada".

2. Garantes de la Seguridad y del ejercicio de derechos y libertades

Actores principales en la aplicación práctica de las medidas concretas que los decisores políticos adoptan son los servicios de inteligencia y las agencias encargadas de la aplicación de la ley[28]. Los primeros, más centrados en la prevención del delito y los segundos -aunque también- en la investigación, la persecución y el enjuiciamiento de conductas y hechos delictivos.

Es muy pertinente, y estamos de acuerdo con ello, hacerse la pregunta que Marsal Muntalá (2005; 221)[29] plantea al respecto [sobre los servicios de inteligencia, pero igualmente válida para los miembros de las Fuerzas y Cuerpos de Seguridad del Estado]: *"¿hasta qué punto deben tener márgenes de actuación que incidan sobre el ejercicio de libertades y derechos de los ciudadanos para garantizar más información que permita mayor prevención?"*. A esta pregunta añadiremos a continuación: *"¿o para garantizar más información que permita mayor capacidad de actuación en un ámbito judicial de persecución del delito?".*

Tampoco es este un debate nuevo, pero igualmente recurrente cada vez que se plantean las discusiones sobre los límites a las capacidades y funciones que estos actores deben ejercer a la hora de garantizar la seguridad de la ciudadanía, sin

[28] Los denominaremos de forma indistinta como agentes encargados de la aplicación de la ley, servicios policiales o fuerzas y cuerpos de seguridad. Con esta denominación, aunque no se precise, nos referiremos a las de carácter estatal, excluyendo a las autonómicas y locales, por cuanto puede haber limitaciones en cuanto a las funciones que, en la materia objeto de estudio, pueden realizar en el ámbito de la investigación penal. No obstante, a los efectos de nuestro ámbito de investigación es, en cierto modo, irrelevante.

[29] MARSAL MUNTALÁ, J., *"Seguridad versus Libertad…", op. cit*. 221.

menoscabo de sus derechos y el ejercicio de sus libertades. Y también aquí, como en casi todo en la vida, influyen la experiencia previa y otros condicionamientos de tipo ideológico. Aun así, sigue siendo necesario, como también lo es dejar de lado al menos las cuestiones puramente ideológicas. La experiencia siempre será bienvenida a la hora de aportar conocimiento y propuestas de mejora.

A ese respecto, surgen también preguntas sobre la eficacia de las investigaciones penales -dejamos de lado por ahora la labor preventiva- en un mundo en el que cada vez se ponen a disposición del individuo más herramientas tecnológicas y de las comunicaciones y del tratamiento de la información (que son aprovechadas también por delincuentes y Estados con fines delictivos) y, al mismo tiempo, se establecen más y más potentes garantías al ejercicio de derechos y libertades, pero que no permiten un aprovechamiento igualmente amplio por quienes están llamados a preservar algo tan básico como la vida de las personas. Surgen preguntas sobre si se deben establecer límites al ejercicio de esos derechos y en qué medida; surgen preguntas sobre cómo cumplir con los criterios de proporcionalidad, necesidad y oportunidad; surgen preguntas sobre si se puede establecer alguna legislación que permita conjugar todos los intereses, y si esta debe ser a nivel nacional o no cabe otra opción que buscarla a nivel internacional -o de la Unión Europea, para el caso que nos ocupa.

Adelantamos que es un debate en el que probablemente podamos encontrar quienes responderán que es posible y necesario; hasta quienes aboguen por otros métodos igualmente eficaces, pero menos lesivos de derechos; o quienes se decanten claramente en favor del libre ejercicio de derechos sin límite alguno. En cualquier caso, uno de los objetivos fundamentales de esta tesis es llegar a contestar al menos a alguna de estas preguntas, en un ámbito concreto que se especificará a lo largo de los siguientes capítulos, pero que consideramos de extraordinaria relevancia presente y futura para la Unión Europea y para la seguridad de sus ciudadanos. La primera respuesta que nos viene al recuerdo -y valga una expresión poco académica para un trabajo de estas características- es una frase que hace años oímos como respuesta a una persona que quería hacer un regalo y buscaba algo que reuniera las características de ser actual/moderno, grande y bonito, pero muy barato: *"manzanas grandes y que pesen*

poco". La conclusión que queremos expresar es: no es posible, no existe. Hemos de conseguir ceder en ambos lados para obtener el mejor producto que permita establecer ciertos límites y garantizar un nivel de seguridad aceptable. A buen seguro, no cerrará el debate inconcluso entre *"Libertad vs. Seguridad"*, pero esperamos que contribuya a matizar las posiciones y a avanzar hacia un mejor entendimiento entre quienes seguirán defendiendo una u otra postura.

Los servicios de inteligencia y las fuerzas y cuerpos de seguridad son unos de los principales *"instrumentos"* con los que cuentan los Estados para garantizar la Seguridad y, de esa forma, para garantizar también el libre ejercicio de las libertades y el pleno disfrute de los derechos y, con ello, mantener los estándares democráticos exigibles a cualquier país.

Una de las medidas controvertidas, y que afecta a la labor de los servicios policiales y de inteligencia como parte de su contribución a la seguridad de un país, es la recogida y tratamiento de información de muy diverso tipo y de muy variadas y amplias procedencias. Y es esta una de las que nos interesa sobremanera por cuanto está cada vez de mayor actualidad. Hay quienes consideran que se tiende hacia una ampliación de la recogida de información a disposición del Estado bien porque afecta a un número cada vez mayor de personas o porque afecta a una cada vez más amplia categoría de datos. En ese sentido, respecto de la Directiva europea de conservación de datos a la que ya nos hemos referido antes, Rodotà (2006; 56)[30] asevera que:

> *"existe una tendencia más general hacia la extensión de la recogida de información a un número cada vez mayor de personas. Se pasa de la recogida con miras a la recogida generalizada. Se amplía el área de las personas sometidas a control. Ya no sólo personas solas o grupos considerados peligrosos; en este momento la población entera está considerada como 'potencialmente peligrosa' que justifica la creación de la recogida total de datos y la incesante producción de perfiles individuales, familiares, de grupo, basados en informaciones que atañen también a la salud, a la situación financiera y a las elecciones culturales"*.

[30] RODOTÀ, S., *"La conservación de los datos de…", op. cit.* p. 56

Añade también la posibilidad de interconectar diferentes bases de datos y sistemas de las que disponen los poderes públicos, como elemento que aporta gravedad a la situación. Sin embargo, obvia que cada uno de esos sistemas de información está creado en base a criterios de acceso particulares y que su interconexión solo puede ser viable si existe una norma legal que así lo determine, y para los casos concretos establecidos en la ley. En consecuencia, el Estado no puede actuar con arbitrariedad y sustrayéndose a la ley, para hacer lo que *quiera o le venga en gana*. Rodotà (2006; 57)[31] considera que la multitud está ya *"desnuda"* y cita el oxímoron *"emergencia permanente"* como una excepción que se extiende de forma permanente y se convierte en una *"verdadera y estable disciplina de futuro"*.

Pero, a mayor abundamiento, se extiende la sospecha sobre la posible actuación de los investigadores policiales al hecho de poder *"malinterpretar"* la información conservada y darse el caso de que, por ejemplo, un número de reiteradas llamadas fallidas con un interlocutor que sea posteriormente objeto de investigación por la comisión de un delito grave pueda dar lugar a la imputación/investigación también del inocente que ha efectuado o, incluso recibido, esas llamadas.

Aunque no hemos entrado si quiera a precisar el tipo de datos (la información) sobre la que centraremos nuestra investigación, ni hemos comenzado el análisis jurídico correspondiente a la implantación de las medidas para su almacenamiento, que posteriormente fueron declaradas contrarias a Derecho por la jurisdicción europea, citaremos, por ser pertinente en este momento, el Caso Malone, que da nombre a la Sentencia del Tribunal Europeo de Derechos Humanos (TEDH) de 2 de agosto de 1984[32], relativa al registro policial de conversaciones telefónicas, dirigida por James Malone contra el Reino Unido, al amparo del artículo 25 del Convenio para la protección de los Derechos Humanos (CEDH). En este caso, el Tribunal de Estrasburgo admite que *"Sin embargo, el ejercicio de semejantes facultades crea [las escuchas para investigar y combatir los delitos], por su naturaleza secreta, el riesgo de abusos, fáciles de cometer en casos individuales y propicios a consecuencias perjudiciales para el*

[31] *Ibíd.*, p. 57.

[32] Sentencia TEDH 8691/79, de 2 de agosto de 1984, relativa al registro policial de conservaciones telefónicas.

conjunto de la sociedad democrática… Por consiguiente, la intervención que se produce sólo puede considerarse 'necesaria', 'en una sociedad democrática', si se rodea el sistema de vigilancia adoptado de garantías suficientes contra los abusos"[33]. Analiza este caso González de la Garza (2004; 272)[34] al tratar ¿qué son los datos de tráfico y facturación?[35], y nos recuerda que, si bien estos datos deberían ser borrados una vez que hayan cumplido su finalidad, la utilidad patrimonial para las organizaciones que los recogen relativiza la eficacia de esa medida, lo que entendemos que ofrece alguna opción a prácticas como las que enjuició el TEDH en el Caso Malone. Por su parte, al estudiar García Sanz (2011; 153)[36], las redes sociales en línea, se pregunta si pueden ser consideradas como fuentes de acceso público o ficheros de datos personales privados, lo que muestra cómo los avances tecnológicos obligan a repensar argumentos y conceptos sobre los que ya había gran consenso. En ese sentido, la autora concluye que *"dado el elenco de excepciones y exenciones que asisten al usuario [de redes sociales], que confieren plena legitimidad al ejercicio libre del derecho a la información, expresión o de creación literaria, científica o técnica, estos espacios parecen más próximos a su consideración como fuentes públicas de información, desde el punto de vista de la legislación de protección de datos, que como ficheros privados de datos personales … lo que no justifica la desprotección, pero sí un régimen jurídico diferente"*. E incluso respecto de los diferentes tipos de datos, hay autores (2009; 207)[37] que analizaban la normativa europea de conservación de datos y observaban *"la necesidad de delimitar bien los datos concretos a los que debe extenderse el secreto, diferenciándolos de aquéllos que forman parte del contenido del derecho a la protección de datos o de los que deberían protegerse a través del derecho a la intimidad"*.

Ya observó el Tribunal de Derechos Humanos la lesión del artículo 8 del CEDH -lo abordaremos más adelante- al corroborar que se habían puesto a disposición de la

[33] Fundamento 84 de la sentencia 8691/79.

[34] GONZÁLEZ DE LA GARZA, L.M., *Comunicación Pública en Internet*, Creaciones Copyright, Madrid, 2004, p. 272.

[35] Estos datos serán una parte de los que trataremos a lo largo de nuestra investigación, que tanto en el momento en que se dictó la sentencia al Caso Malone, como ahora -ampliados- son fundamentales en las investigaciones penales.

[36] GARCÍA SANZ, R.M., *"Redes sociales online: fuentes de acceso público o ficheros de datos personales privados (Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas)"*, 2011, Revista de derecho político, UNED, nº 81, 2011, pp. 101-154, p. 153.

[37] LÓPEZ BARAJAS, I., "*El deber de conservación de datos en la Unión Europea y sus límites",* en Revista de Derecho de la Unión Europea, nº 16, 2009, pp. 195-220, p. 207.

Policía datos conservados para otros fines sin consentimiento del afectado. Analizan Cubero Marcos y Aberasturi Gorriño (2008; 194)[38] esta circunstancia, respecto de la Ley 25/2007 sobre conservación de datos, poniendo de manifiesto el desamparo en que se sitúa a los ciudadanos al no ser advertidos por los operadores de telecomunicaciones de que sus datos han sido conservados para la persecución de delitos graves, la criminalidad organizada o de grupos terroristas.

Por otro lado, no podemos obviar que, en el marco de una investigación pudiera producirse una situación de esas características, pero no olvidemos que, de contar únicamente con esos elementos de valoración, no habría otro fin que el que descartar la sospecha sobre esa persona inocente. Es sabido que los datos que se puedan obtener y tratar de esta forma, constituyen elementos que se suman a otras pruebas o indicios igualmente importantes que van dando forma a la investigación. No obstante, reiteramos que entendemos, aunque no compartimos, que se pueda tener esa *sospecha/miedo* respecto de la quiebra del principio de presunción de inocencia.

3. La información como elemento imprescindible

"Información es poder". Esta es una frase muy repetida antiguamente entre quienes formaban parte de los servicios policiales o de inteligencia, pero después también en el mundo financiero, y hoy día en casi todos los ámbitos de la vida. Es cierto que cada vez hay más *Open Source Intelligence* (OSINT)[39] que, adecuadamente tratada (de forma individual o a través de herramientas que se ponen a disposición de cualquier usuario dispuesto a gastar un poco de dinero), pueden aportar ventajas competitivas respecto de los demás, bien para protegerse o para tomar decisiones que otorguen una posición de privilegio para quien la posee. No obstante, otro tipo de información no tan accesible al público general es igualmente importante -en ocasiones fundamental- para obtener pruebas con garantías suficientes para el ejercicio posterior de la justicia, en el esclarecimiento y enjuiciamiento de delitos graves. Es en este segundo ámbito en el que

[38] CUBERO MARCOS, J.I., y ABERASTURI GORRIÑO, U., *"Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007, sobre conservación de datos"*, Revista Española de Derecho Constitucional, nº. 83, 2008, pp. 175-197, p. 194.

[39] Habitualmente se utiliza el término en inglés para referirse a la inteligencia de fuentes abiertas, que hace referencia al conocimiento recopilado a partir de fuentes de acceso público. Para profundizar, vid. https://www.incibe-cert.es/blog/osint-la-informacion-es-poder.

se plantea la dicotomía entre Seguridad y Libertad en el disfrute de derechos y en el ejercicio de las libertades públicas.

La actividad de los servicios policiales y de inteligencia en un estado democrático está sujeta a controles. Parece una afirmación innecesaria, por obvia; no obstante, en no pocas ocasiones se cuestiona. Se establecen controles administrativos y judiciales, que garantizan una actuación adaptada a derecho y, en caso contrario, existen mecanismos de corrección y reparación del daño causado. Por citar el caso español, tenemos un sistema muy garantista con el ejercicio de los derechos y las libertades, de forma que se exige autorización para la mayoría de las actuaciones que los agentes encargados de hacer cumplir la ley llevan a cabo.

Pero, adelantando parte del contenido del objeto de investigación y dando un salto hacia el objeto concreto de este estudio, es decir, los datos de que disponen los proveedores de servicios de telecomunicaciones, y el cambio de situación respecto de su uso y tratamiento por las agencias encargadas de aplicar la ley producido como consecuencia de sucesivas sentencias del Tribunal de Justicia de la Unión Europea, nos planteamos otra pregunta acerca de si, un sistema garantista como el español -o el del resto de Estados miembros- en un momento de avances tecnológicos que han eliminado las fronteras en el intercambio de información entre usurarios -aprovechado también por delincuentes- garantiza la eficacia del trabajo que éstos realizan en favor de la Seguridad y la protección de los ciudadanos y en la persecución y enjuiciamiento de los delitos graves. O, por el contrario, ¿resta eficacia a esa labor? Y, en caso negativo, ¿se pueden encontrar alternativas que permitan mantener la eficacia en niveles adecuados sin menoscabar los derechos y las libertades? Afirma Ortiz-Pradillo (2013; 335)[40] que la tecnología debe ser usada también al servicio de la investigación criminal, de la misma forma que se usa en otros ámbitos profesionales, pero *"no es posible justificar el empleo de cualesquiera métodos de investigación, sin una mínima base legal que regule sus garantías, requisitos, límites, bajo la excusa de poder contrarrestar así los avances con los que cada día cuentan los criminales para cometer sus delitos"*. Estamos de

[40] ORTIZ-PRADILLO, J.C., *"El impacto de la tecnología en la investigación penal y en los derechos fundamentales",* en Problemas actuales de la justicia penal, Madrid, 2013, pp. 317-341, p. 221.

acuerdo con ello; no obstante, no se nos ocurren situaciones actualmente en las que esto pudiera ser así en la Unión Europea.

Asevera Marsal Muntalá (2005; 221)[41] que *"pensar que las restricciones de libertades y derechos permiten una mayor seguridad en el mundo actual es una equivocación, pues ello solo da la seguridad de que tenemos menos libertades y menos derechos"*. A priori, en este momento del estudio no podemos estar de acuerdo con el autor. No obstante, cuando lleguemos al final del recorrido que iniciamos, esperamos estar en disposición de aportar argumentos a favor del desacuerdo o, quién sabe, quizás otros que nos hagan sumarnos a su tesis. Por el contrario, sí estamos a favor de su otra consideración, relacionada solo con los servicios de inteligencia, pero igualmente válida para las fuerzas y cuerpos de seguridad, acerca de la importancia de estos y de su eficacia como elemento influyente en el equilibrio entre seguridad y libertad y derechos. No obstante, una vez más, lo difícil es pedir eficacia aun cuando estos no disponen de medios suficientes que avancen al mismo ritmo que aquellos de los que disponen los delincuentes; en algunas circunstancias conseguidos mediante el aprovechamiento de herramientas creadas para favorecer al ciudadano y garantizar su privacidad e intimidad, pero cuya tenencia y uso son sustraídos a quienes trabajan para protegerles. Aun así, estamos de acuerdo con González de la Garza (2004; 278)[42] respecto de que *"... en una sociedad democrática la defensa de la intimidad de las personas es un presupuesto ineludible de la libertad"*, y esto exige, como también expresa el autor -al referirse a la mayor concienciación con la delincuencia informática-, no encontrar excusas para dejar de buscar con ahínco otras alternativas a la estrecha vigilancia de los ciudadanos. Rebollo Delgado (2020; 29)[43] reconoce también el poder que constituyen los datos y su facilidad de tratamiento, así como los aspectos positivos y negativos sobre los ciudadanos de los avances tecnológicos, pero pone acertadamente en la balanza, a nuestro modo de ver, el riesgo que corren tanto los ciudadanos como el Estado por el uso abusivo o incontrolado de los datos.

[41] MARSAL MUNTALÁ, J., *"Seguridad versus Libertad…"*, *op. cit*. p. 221

[42] GONZÁLEZ DE LA GARZA, L.M., Comunicación Pública en…, *op. cit*. p. 279.

[43] *"Encuesta sobre la protección de datos personales"*, Teoría y Realidad Constitucional, 46, 2020, pp. 15-118, p. 29, en https://www-proquest-com.bibliotecauned.idm.oclc.org/scholarly-journals/encuesta-sobre-la-protección-de-datos-personales/docview/2535570794/se-2

Indicaba Rodotà (2006; 56), respecto del entonces recientemente aprobado texto de la Directiva de conservación de datos, que establecía o reafirmaba un *"poder absoluto del Estado"* sobre los datos generados por determinadas comunicaciones electrónicas de los ciudadanos y consideraba que habría que reivindicar lo que llama un *"habeas data"* similar al habeas corpus, pero en este caso aplicable al *"cuerpo físico", "reaccionando así a las pretensiones absolutistas del rey*. Es cierto que en el momento de redacción de estas aseveraciones -el año 2006- se acababa de aprobar la Directiva en cuestión y que el TJUE le ha dado la razón en cierto modo; pero, aun así, no compartimos que la pretensión inicial fuera de esa índole ni con esa intensidad. No obstante, nos parece interesante la idea de un *"habeas data"*, de cara a las consideraciones finales a las que nos pueda llevar esta tesis. Pérez Luño (1990; 155)[44] se refiere a un movimiento de la doctrina jurídica y de la jurisprudencia que ya en el aquel momento se estaba generando en los países con más desarrollo tecnológico *"tendente al reconocimiento del derecho a la libertad informática y a la facultad de autodeterminación en la esfera informativa, que tiene su principal instrumento de garantía en el Habeas Data, es decir, en la facultad de las personas de conocer y controlar las informaciones que les conciernen procesadas en bancos de datos informatizados"*.

4. La Unión Europea en la lucha contra las amenazas graves a su seguridad

El título del epígrafe ya indica los límites geográficos fundamentales del trabajo. Si bien, podríamos y quizás deberíamos estudiar también lo que se ha hecho en otras partes del mundo como, por supuesto, EE. UU., lo que realmente nos interesa es conocer las medidas adoptadas en la Unión Europea, puesto que ambas áreas geográficas difieren en la incardinación de esas medidas en el ordenamiento jurídico propio -en ocasiones de forma notable- y porque el objeto principal de estudio se circunscribe al espacio europeo, pues es ahí donde se adoptó la Directiva de 2006 que centra nuestro trabajo. Una mirada más alejada podría ser interesante, sin duda, pero probablemente no aportaría soluciones prácticas al problema que queremos estudiar, por cuanto la legislación europea en materia de protección de determinados derechos

[44] PEREZ LUÑO, A.E. *"Del habeas corpus al habeas data"*. Conferencia impartida el 11 de mayo de 1990, XIV Curso de Informática y Derecho, Centro Regional de la UNED de Extremadura. Curso sobre Informática y Derecho, 1990, pp. 153-161, p. 155.

fundamentales, especialmente respecto de la protección de los datos personales, es considerada de las más garantistas del mundo, y eso tiene consecuencias particulares. En consecuencia, no parece fácil encontrar soluciones que cumplan con ese criterio fuera de la Unión Europea. Somos conscientes de que es una afirmación pretenciosa que renunciamos a contrastar con hechos, pero no creemos que se pierdan elementos importantes que aplicar a la solución europea que aquí pretendemos al menos esbozar. Aun así, habrá referencias concretas a otros países en aspectos concretos de nuestra investigación[45].

Partiremos de una premisa: la inmensa mayoría de los ciudadanos europeos no cuestionan que la Unión Europea y, por extensión, cada uno de sus Estados miembros, están vinculados por el derecho internacional relativo a los Derechos Humanos, tal y como vienen recogidos en la CDFUE. En consecuencia, el respeto a estos derechos en cada una de las medidas que se adoptan para luchar contra las amenazas graves a su seguridad -pongamos por ejemplo una de las más graves, la que provoca el terrorismo yihadista- está garantizado.

En el caso concreto citado del terrorismo yihadista -pero también en el de cualquiera otra amenaza- las medidas que se adopten y las acciones que se pongan en funcionamiento ya no pueden ser nacionales o domésticas; se necesitan estrategias globales y comunes, cuyo único límite es la consideración de los Derechos Humanos y Fundamentales[46]. Sin embargo, según Serra Cristóbal (2014; 18)[47], se ha optado por el camino inverso; es decir, por la adopción de medidas extraordinarias a criterio de cada

[45] Además de EE. UU., también a Canadá, Japón o Australia. O un país, ahora tercer Estado respecto para la Unión Europea, pero que hasta hace poco tiempo era un miembro más del *club* comunitario, aunque siempre ha sido muy particular: el Reino Unido.

[46] El Parlamento Europeo y el TJUE han cuestionado precisamente las medidas de política contra el terrorismo y el respeto de los derechos de los individuos. Por citar algunos ejemplos: Resolución del Parlamento, de 15 de diciembre de 2005, sobre la presunta utilización de países europeos, por parte de la CIA, para el transporte y la detención ilegal de presos (DO C 286 E de 23.11.2006, p. 509);

Decisión, de 18 de enero de 2006, por la que se constituye una comisión temporal sobre la presunta utilización de países europeos por la CIA para el transporte y la detención ilegal de presos (DO C 287 E de 24.11.2006, p. 159); o

Resolución, de 6 de julio de 2006, sobre la supuesta utilización de países europeos por la CIA para el transporte y la detención ilegal de presos.

[47] SERRA CRISTOBAL, R., *"El impacto de las medidas de seguridad antiterroristas en los derechos fundamentales: La necesidad de normas comunes supranacionales de protección de derechos para responder al riesgo de terrorismo"*, en *IX Congreso Mundial de Derecho Constitucional, "Desafíos constitucionales: globales y locales*", Oslo, 16-20 de junio de 2014, p. 18.

país, que han supuesto injerencia y limitación de derechos. Cita Rizzo (2019; 154)[48] como ejemplos: modificaciones en los regímenes de emergencia o en las normas contra el terrorismo o, como el caso de Francia, en la modificación de la propia Constitución.

Como mencionábamos antes, en la Unión Europea, el sistema de seguridad [desde el punto de vista legal] y su aplicación se reservan a cada uno de los Estados miembros[49]; aun así, son constantes las iniciativas jurídicas principalmente de la Comisión Europea, tendentes a buscar una mayor eficacia en la lucha contra estas amenazas -algunas de las cuales veremos a continuación- y hacia una mejor cooperación policial y judicial en materia penal, de acuerdo con lo previsto en el Título V del Tratado de Funcionamiento de la UE, que recoge las disposiciones correspondientes al ELJS. Para Moreno Catena (2013; 51 y ss.)[50], en el orden penal, la cooperación judicial es un verdadero presupuesto para alcanzar la Justicia, especialmente cuando se trata de asuntos transfronterizos, que requiere de la actuación de todos los Estados implicados, de forma que evite el movimiento impune de los delincuentes cruzando fronteras que ya no existen. No obstante, Schünemann (2006; 24)[51] cree que los avances se están produciendo poniendo el acento sobremanera en la represión penal y en menor medida en la salvaguarda de las garantías procesales.

En materia de terrorismo, el artículo 222 del TFUE refuerza la cooperación, al establecer una *"cláusula de solidaridad"*[52] que exige la acción concertada de todos los Estados miembros ante un ataque terrorista a uno de ellos y que, en la práctica [por desgracia], hace que ante cualquier atentado de los cometidos en suelo europeo en los últimos años se convoque a los ministros de Interior de la Unión Europea para la adopción de medidas que básicamente se traducen en un primer momento en una declaración de condena y de muestra de unión y firmeza de los valores europeos ante

[48] RIZZO, G., *"Derecho a la privacidad y seguridad en …"*, *op. cit*., p. 154.

[49] Art. 72 del TFUE.

[50] MORENO CATENA, V., *"El cambio de paradigma y el principio de reconocimiento mutuo y sus implicaciones. Perspectivas del Tratado de Lisboa"*, en Escuela Judicial, Consejo General del Poder Judicial, 2013, pp. 1-57, p. 51 y ss.

[51] SCHÜNEMANN, B. *"¿Peligros para el estado de derecho a través de la europeización de la administración de justicia penal?",* en Armenta Deu, T. (Coord), *El Derecho procesal penal en la Unión Europea. Tendencias actuales y perspectivas de futuro*, ed. Colex, 2006, pp. 19-36, p. 24.

[52] Art. 222 del TFUE, recoge la actuación conjunta con espíritu de solidaridad si un Estado miembro sufre un ataque terrorista, entre otros supuestos.

quienes quieren poner en jaque la pacífica convivencia. Habitualmente, después se insta a la Comisión Europea a adoptar medidas más concretas y prácticas, aunque no solo tiene protagonismo esta institución europea, sino que el papel del Parlamento Europeo y del Consejo de la UE son también imprescindibles y muy relevantes.

Por lo tanto, la política de la Unión Europea en materia de prevención y lucha contra el fenómeno terrorista, pero también en otros ámbitos de seguridad o de lucha contra la delincuencia grave, se articula en base a la armonización de las legislaciones nacionales y el reconocimiento mutuo de resoluciones judiciales[53], aunque siga siendo de competencia estatal y con pocos controles a nivel de la Unión Europea[54]. Algunos autores observan que, a pesar de la armonización, los Estados miembros pueden aducir que el intercambio de información puede ser contrario a los intereses nacionales y no llevarlo a cabo, aunque se haya adoptado una medida para favorecerlo[55]. Esta cláusula, que podemos denominar de *exclusión*, se utiliza frecuentemente para no compartir la información entre servicios policiales y de inteligencia, por falta de confianza en el buen uso de la información por aquellos a quienes se remite y por *miedo* a que pueda desbaratarse alguna investigación relevante, quizás [y es una consideración estrictamente personal] por un malentendido celo profesional o de consideración excesiva de la eficacia y buen hacer de los servicios de investigación de un determinado Estado miembro, en detrimento de los del resto de miembros de la Unión Europea. Etxeberria Guridi (2009; 352)[56] arguye que la causa de que no se haya desplegado todo el potencial del reconocimiento mutuo de resoluciones judiciales está en la gran diversidad de sistemas penales, la diferencia de órganos que participan en ese proceso y

[53] En los últimos años hemos conocido célebres casos de incumplimiento de este principio de reconocimiento de las resoluciones judiciales entre Estados miembros, como las correspondientes a solicitudes dirigidas por España a Bélgica. No obstante, no son las únicas. En fechas muy recientes se ha conocido el Dictamen del Abogado General de la UE respecto de una de las cuestiones prejudiciales planteadas por un juez español y que, de ser seguido por el TJUE, supondrá, sin duda, un avance notable en la determinación de un criterio jurídico en esta materia concreta de reconocimiento de decisiones judiciales a nivel de la Unión Europea.

[54] Para profundizar en la ligazón de la seguridad con el ámbito de los Estados miembros, vid. RIDAURA MARTÍNEZ M.J., *"La seguridad ciudadana como función del Estado"*, Revista de Derecho Público, vol. 62 (2) Estudios de Deusto, 2014, pp. 319-346.

[55] Decisión, de 24 de junio de 2014 relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad (2014/415/UE), artículo 8.

[56] ETXEBERRIA GURIDI, J.F., *"Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo"*, Eguzkilore, nº. 23, San Sebastián, diciembre 2009, pp. 351-366, p. 352.

en la propia estructura de los procesos penales y, para superar estas barreras, se ha de trabajar en la confianza mutua entre los Estados miembros.

Una vez más tenemos que fijarnos en el 11-S como fecha de partida para una mayor concienciación y acción hacia una política común de lucha contra el terrorismo a la que ha seguido grandes avances en este campo. En materia de justicia e interior, en 2009 se aprobó el Programa de Estocolmo para elaborar una Estrategia de Seguridad Interior (ESI), que analiza amenazas y desafíos a los que se enfrentaba en aquel momento la Unión Europea y define objetivos y estrategias hacia un modelo de seguridad europeo, aunque no concreta las competencias que corresponden a una y a los otros; en consecuencia, se asemeja más a un modelo de cooperación entre estados en materias específicas. De forma concreta, recoge que *"la UE debe consolidar un modelo de seguridad basado en los principios y valores de la Unión: el respeto a los derechos humanos y a las libertades fundamentales, el Estado de Derecho, la democracia, el diálogo, la tolerancia, la transparencia y la solidaridad"*[57].

Los atentados de París de 2015 y de Bruselas de 2016 marcaron otro hito importante en cuanto a la revisión de numerosas políticas en materia de seguridad y llevaron a las instituciones europeas a proponer iniciativas para reforzar la seguridad de la Unión, fundamentalmente en materia de prevención antiterrorista, pero también de gestión fronteriza, además de acelerar otros expedientes que llevaban tiempo parados o avanzaban a un ritmo lento. A modo de ejemplo, podemos citar la adopción de la Directiva 2016/680, de 27 de abril, sobre el tratamiento de datos por las autoridades en el ámbito de la prevención y persecución del crimen[58] que, junto con el Reglamento

[57] Para profundizar, vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura, que propone acciones para la implementación de la estrategia durante el periodo 2011-14 (COM/2010/0673 final).

[58] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril, 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 del Consejo 2008/977/JAI. Entró en vigor el 5 de mayo de 2016.

correspondiente[59], dieron lugar al conocido como *"paquete de protección de datos de la UE"*.

Tanto en la lucha antiterrorista como en la lucha contra la delincuencia grave, la necesidad de cooperación entre países es un elemento clave, basado en el intercambio de información y en el acceso a los datos disponibles, allá donde estos estén. Eso hace también que los problemas respecto del acceso y tratamiento de esa información sea común, máxime cuando el anteriormente mencionado *paquete de protección de datos de la UE* ha armonizado las reglas de juego y, en muchas ocasiones, lo ha dificultado. Debemos felicitarnos de que la Unión Europea cuente con una de las legislaciones más avanzadas en materia de protección de las personas [de los ciudadanos europeos] respecto del tratamiento de los datos personales, pero debemos exigir también que no se genere un desequilibrio desproporcionado en los medios que permitan garantizar también otros derechos igualmente importantes.

[59] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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. Entró en vigor el 5 de mayo de 2016.

CAPÍTULO II. EL DERECHO A LA PRIVACIDAD Y A LA PROTECCIÓN DE LOS DATOS EN EL AMBITO DE LA POLICÍA Y LA JUSTICIA PENAL

Muchos autores sitúan la aparición de la protección de los datos de carácter personal en 1890, en los Estados Unidos, por la confluencia de varios sucesos; el más importante de ellos es la publicación del imprescindible artículo de Samuel D. Warren y Louis D. Brandeis[60], *The Right to Privacy* [El derecho a la intimidad], en diciembre de ese año[61], que defendía que debía concederse protección jurídica a la intimidad, partiendo de los principios consagrados en la *Common Law*. Lo ciertamente relevante del artículo[62] fue el seguimiento masivo que de forma rápida se hizo por parte de jueces y legisladores en los Estados Unidos, cuando hasta ese momento solo había habido manifestaciones puntuales y fragmentadas. Es cierto que no fueron los únicos autores que también en esos mismos momentos apostaban por lo mismo. El elemento común a todos ellos es el momento histórico que viven: el esplendor de la Segunda Revolución, que trajo un rápido desarrollo tecnológico propiciado por la electricidad y, al mismo tiempo, la culminación del individualismo propio del hombre moderno. De forma concreta, lo que movió a estos dos socios a escribir el artículo fue la percepción de la súbita amenaza de las muy nuevas tecnologías de la información y, de forma particular, el uso abusivo de las mismas por el incipiente periodismo de masas. Fuere como fuere, de forma unánime, el mundo jurídico norteamericano lo considera como el verdadero punto de partida del reconocimiento del derecho a la intimidad.

El paso disruptivo del artículo de estos dos socios está en que razonan acerca de que el Derecho puede y debe proteger no solo la propiedad y la reputación, como había venido haciendo hasta ese momento, sino también los pensamientos, sentimientos y emociones *(thought, sentiment and emotions)*, es decir, la personalidad inviolable

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

[61] WARREN, S.; BRANDEIS, L., The right to privacy, *Harward Law Review* (15 de diciembre de 1890), vol. 4, nº. 5, p. 193-220.

[62] Para profundizar sobre la importancia de este artículo, como origen de la protección de la privacidad en Norteamérica, vid. NIEVES SALDAÑA, M., NIEVES SALDAÑA, M., *"The right to privacy: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis"*, UNED, Revista de Derecho Político, núm. 85, 2012, pp. 195-240.

(inviolate personality), basándose en que, de la misma forma que el *Common Law* se ha ido adaptando a lo largo de los tiempos para garantizar la protección del ciudadano y sus bienes, cuando surgen nuevas circunstancias [como son los avances tecnológicos y su influencia en la vida de las personas], se debe evolucionar también para ofrecer protección a las personas contra los ataques [en este caso concreto de los ataques de los medios de comunicación de masas], no siendo suficiente con la protección de la reputación (que consideran la dimensión externa y social del hombre), sino también de su ámbito reservado y propio, de sus ideas y sus pensamientos más íntimos; lo que Brandeis y Warren llaman *"privacy"*. Además, pronto se conectó este nuevo derecho con las normas de los derechos fundamentales de la Constitución norteamericana y los tribunales comenzaron a citar expresamente *The Right to Privacy* en sus sentencias y a reconocer como derecho natural inalienable el disfrute y la defensa de la vida y la libertad, la adquisición, la posesión y la protección de la propiedad y la persecución y obtención de la seguridad y la felicidad *("... have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing and protecting property; and pursuing and obtaining safety and happiness")*. Los jueces identificaban esta situación, independientemente del nombre que se le asigne, con el respeto del espacio privado que no debe ser invadido de forma consciente y sin motivo alguno que lo justifique.

En Europa, en fechas muy próximas a la publicación de Brandeis y Warren, algunos autores alemanes comenzaron a teorizar también sobre los derechos de la personalidad y la necesidad de su protección jurídica, que incluía también en cierto modo la esfera privada del individuo. No fue pacífica la doctrina en este ámbito, pero no profundizaremos en esta discusión doctrinal inicial, por cuanto nos interesa más exponer el momento en el que se consolida como tal. Lo cierto es que la aparición de avances tecnológicos (como la fotografía) encaminó la discusión en un sentido parecido a lo ocurrido en Estados Unidos, de forma que se comenzó a plantear de qué modo podría protegerse la imagen de las personas contra la difusión y la explotación de fotografías tomadas a las personas, lo que dio lugar a que se propugnara un derecho general a la personalidad, bajo el argumento de que la imagen forma parte del derecho a la integridad personal.

Otros países europeos donde se comenzó también a tratar esta misma cuestión fue Suiza, donde se hizo un reconocimiento innovador del derecho general de la personalidad. En Francia, ya en 1909 se traslada al derecho francés este concepto. En Italia, se produce de forma general en las décadas de los 30 y 40 del siglo pasado. En España, aunque de forma más retrasada que otros países europeos [como en tantas otras cuestiones], se recogió este derecho principalmente mediante la jurisprudencia del Tribunal Supremo (TS), que ya en 1912 enjuició el caso de una noticia periodística de una persona que se fugó y posteriormente se suicidó; información que se comprobó que era falsa. Pero, por derecho de la personalidad, se suelen incluir también el respeto a la vida, la integridad corporal, la libertad, los bienes individuales y sociales, el honor y la fama, la intimidad personal, la imagen, el reconocimiento de la cualidad de autor, el nombre, etcétera.

En el mundo actual, las sociedades dependen en gran medida del uso de las tecnologías de la información y las comunicaciones (TIC) y de la creación de productos y servicios cada vez más asequibles a los ciudadanos, que crean nuevas formas de relacionarse y comunicarse. Los datos que generan estas tecnologías y su uso nos afectan todos los días y de muchas formas diferentes, hasta el punto de que la economía mundial está basada cada vez más, al menos en algunos de sus pilares fundamentales, en el tratamiento de los datos, incluidos los personales.

Estos avances han revolucionado y -aunque nos parezca raro- siguen haciéndolo todos los aspectos de la vida personal, familiar y profesional, facilitando el acceso a la información de una forma cada vez mayor y más rápida. Como consecuencia, también tiene un efecto en las administraciones públicas, en los proveedores de servicios, en los decisores políticos, etcétera, que se ven obligados a cambiar sus sistemas de gestión y de procesado de la información para beneficiar a los ciudadanos y también para beneficiarse ellos mismos. Pero, al mismo tiempo, tienen que prestar especial atención a que el acceso a la información personal de los ciudadanos cumpla con los derechos

fundamentales afectados principalmente: la privacidad y la protección de los datos personales. Como argumenta Geraldes Da Cunha Lopes (2015; 159)[63]:

> *"estamos ante el comienzo de una revolución que va a redefinir el Estado de Derecho y de un cambio en los conceptos de soberanía del Estado como consecuencia de las nuevas preocupaciones por la seguridad internacional y el uso regular de las bases de datos que permiten almacenamiento masivo de información o redes que permiten comunicaciones rápidas y seguras"*.

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

Los datos que los ciudadanos *entregan* a personas y empresas son muy variados y, en muchas ocasiones -nos atreveríamos a decir que en la mayoría de las ocasiones- sin ser conscientes de ello, lo que deriva en la pérdida del control sobre lo que se hace con esa información, máxime cuando son recogidos y tratados por empresas la mayoría de las veces situadas fuera del ámbito geográfico de la Unión Europea; es decir, sometidos a movimientos internacionales con terceros países con normativas y estándares muy variados y distintos a los europeos en cuanto a su protección. No obstante, no estudiaremos aquí esa situación, por cuanto sería inabarcable y más propia de un estudio aparte y específico.

Nuestra *empresa*, respecto de la privacidad y la protección de los datos, partirá entonces de la comprensión de los elementos que configuran los datos personales en el

[63] GERALDES DA CUNHA LOPES, T.M., *"El derecho a la intimidad y la protección de datos en la era de la Seguridad global"*. Principios constitucionales versus riesgos tecnológicos, Anuario Jurídico y Económico Escurialense, nº 48, 2015, pp. 159-180, p. 159

ámbito de la Unión Europea, comenzando con el derecho a la privacidad y la subsiguiente revisión normativa.

El derecho fundamental a la protección de los datos de carácter personal es considerado por Pérez Estrada (2019; 1300)[64] como de *"tercera generación"* e íntimamente ligado al desarrollo de las TIC; en este caso, desde el punto de vista de su incidencia negativa en el ejercicio de los derechos fundamentales. Sigue el término acuñado por Pérez Luño[65], que los define como una generación de derechos que complementa fases anteriores, referidas a las libertades de signo individual y a derechos económicos, sociales y culturales; de forma que los de tercera generación se presentan como respuesta a lo que denomina *"contaminación de libertades" (liberties pollution),* con el que determinados sectores del derecho anglosajón se refieren a la degradación de los derechos fundamentales producida por los usos de las nuevas tecnologías.

Comenzaremos en los próximos párrafos por describir la situación actual, aunque cronológicamente sería más convencional hacerlo desde los comienzos hasta la actualidad. Empero, al margen de que consideramos necesario hacer un balance desde el punto de inicio de la configuración de estos derechos en la Unión Europea, la situación actual es que determina en mayor medida el criterio del Tribunal europeo y la que ha sido tenida en cuenta en la invalidación de la Directiva en torno a la que gira el objeto de estudio de esta tesis.

Desde la entrada en vigor del Tratado de Lisboa, la Carta de los derechos fundamentales de la Unión Europea tiene valor de Derecho primario[66]. Los destinatarios

[64] PÉREZ ESTRADA, M.J., *"La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información"*, Universidad del País Vasco, 2019, en http://orchid.org/0000-0001-7402-4863, consultado el 18 de julio de 2022.

[65] PÉREZ LUÑO, A.E, *"Las generaciones de derechos humanos"*, Universidad de Sevilla, Revista del Centro de Estudios Constitucionales, núm. 10, 1991, pp. 203-207, p. 206.

[66] Vid. artículo 6.1 del Tratado de la Unión Europea (TUE), que otorga a la Carta *"el mismo valor jurídico que los Tratados"*. Véase también, European Union Agency for Fundamental Rights -FRA et al.-, 2018, pp 19-20: *"El Derecho de la UE está compuesto por Derecho primario y Derecho derivado. Los Tratados, en concreto el Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE), han sido ratificados por todos los Estados miembros de la UE y constituyen el Derecho de la Unión Europea. Los reglamentos, Directivas y decisiones de la UE han sido adoptados*

de la Carta son, en particular, las instituciones de la Unión y, por tanto, el Consejo cuando actúa en calidad de legislador, así como los Estados miembros *"únicamente cuando apliquen el Derecho de la Unión"*[67]. Por consiguiente, su inobservancia por parte del legislador de la Unión puede llevar a la anulación por el Tribunal de Justicia del acto de que se trate.

El artículo 8.1 de la Carta dispone que *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"*[68]. Según el Tribunal de Justicia, *"este derecho fundamental se halla íntimamente ligado al respeto a la vida privada, consagrado en el artículo 7"*[69] de la Carta, según el cual *"toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones"*.

El derecho al respeto de la vida privada se recoge en el artículo 8.1 del Convenio Europeo de Derechos Humanos (CEDH)[70] y, en consecuencia, con arreglo al artículo 52.3 de la Carta, tiene el mismo sentido y alcance que el que le otorga el CEDH[71].

Los datos personales solo pueden ser objeto de tratamiento[72] si se respetan determinados principios comunes en dicho ámbito: los principios de lealtad, finalidad,

---

por las instituciones de la UE, en las que se ha delegado tal autoridad en virtud de los Tratados, y constituyen el Derecho derivado de la UE".

[67] Artículo 51.1 de la Carta.

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

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

[70] El Convenio Europeo de Derechos Humanos (CEDH) se firmó en 1950 por el Consejo de Europa y constituye un tratado internacional para proteger los derechos humanos y las libertades fundamentales en Europa. Los cuarenta y siete países que forman el Consejo de Europa, de los que veintisiete son miembros de la UE, se han adherido al Convenio. El Convenio creó el Tribunal Europeo de Derechos Humanos (TEDH), con el fin de proteger a las personas de las violaciones de los derechos humanos. Cualquier persona cuyos derechos hayan sido violados en virtud del Convenio por un Estado parte puede presentar su caso ante el Tribunal. El Convenio cuenta con varios protocolos que modifican su marco. El Tratado de Lisboa permite desde el 1 de diciembre de 2009, que la UE se adhiera al CEDH y en 2013 se ultimó un preacuerdo de adhesión. Para profundizar sobre el CEDH, vid. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:eu_human_rights_convention

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

legitimación, transparencia y control por autoridades independientes, que la Carta formula así:

> Los datos *"se tratarán en modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley"*. Además, *"toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación"* y *"el respeto de estas normas estará sujeto al control de una autoridad independiente"* (artículo 8, apartados 2 y 3, de la Carta)[73].

Sólo pueden aportarse limitaciones al derecho a la vida privada y a la protección de datos si se respetan determinadas condiciones. El artículo 8.2 del CEDH sólo admite una injerencia:

> *"en tanto en cuanto (…) esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de los derechos y las libertades de los demás"*.

Por su parte, el artículo 52.1 de la Carta sólo admite una limitación: que esté establecida *"por la ley y [respete] el contenido esencial de dichos derechos (…) dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando 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"*.

---

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

[73] Esto corresponde, entre otros, a los principios de licitud, proporcionalidad y finalidad previstos en el artículo 5.1.a) del Reglamento General de Protección de Datos de la UE.

Son estas disposiciones las que sirven de marco de análisis al TJUE, que en este ámbito sigue al TEDH para examinar la compatibilidad de una medida de tratamiento de datos con los derechos en cuestión[74].

Una vez observada la injerencia o el menoscabo de los derechos, en aplicación del criterio del TEDH de que *"el simple hecho de memorizar datos relativos a la vida privada de un individuo constituye una injerencia"*[75], deben examinarse las justificaciones de dicha injerencia, lo que implica tener en cuenta tres condiciones acumulativas[76]:

- La injerencia o el menoscabo deben estar previstos por la ley, que ha de entrañar determinadas cualidades de accesibilidad y previsibilidad, en particular un régimen suficiente de control del tratamiento;
- Debe responder a un objetivo de interés general reconocido por la Unión (objetivo legítimo); y
- Debe ser necesaria y responder efectivamente al objetivo de interés general (que supone un control de proporcionalidad).

Cuando se trata de una excepción a derechos fundamentales garantizados por la Carta y el CEDH, las justificaciones de la injerencia exigen *una interpretación estrecha*[77]. El Tribunal de Justicia se pronuncia en el mismo sentido: *"las excepciones a la protección de los datos de carácter personal y las limitaciones de dicha protección deben establecerse sin sobrepasar los límites de lo estrictamente necesario*[78]*"*.

En consecuencia, las medidas previstas en la normativa europea deberán ser analizadas en función de estos criterios a la hora de determinar si se produce un menoscabo o una injerencia en los derechos fundamentales previstos en los artículos 7 y

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

[75] Vid. Sentencia del Tribunal de Derechos Humanos, Marper, 4 de diciembre de 2008, nº 30562/04 y 30566/04, 67.

[76] Vid. punto 62 de la Sentencia Volker antes citada y punto 76 de la sentencia antes citada Österreichischer Rundfunk. Sobre la jurisprudencia del Tribunal de Derechos Humanos, véase citado dictamen del Servicio Jurídico doc. 10146/01.

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

[78] Sentencia Volker antes citada, punto 77.

8 de la Carta y en el artículo 8 del CEDH, y si se reúnen las condiciones que permitían justificar una injerencia[79].

1. Confidencialidad, privacidad/vida privada y protección de datos: complementariedad conceptual

Desde tiempos inmemoriales, a determinadas profesiones se les han asignado reglas o normas que exigían la confidencialidad. De forma automática pensaríamos en el juramento hipocrático de los médicos o en el secreto de confesión de los sacerdotes; pero también podemos recurrir a otras profesiones más recientes y, en ocasiones, asociadas a la sociedad de la información y las telecomunicaciones. En definitiva, se obliga a quienes obtienen información de forma privilegiada, a guardarla y no compartirla con terceros. De esa forma, se genera un clima de confianza hacia las instituciones y los profesionales con los que se comparte información personal y, en su conjunto, se sirve también a la sociedad por cuanto ese clima de confianza puede ayudar a mejorar situaciones concretas, como las de salud pública o de seguridad, entre otras muchas.

Sin embargo, aun con el deber de confidencialidad, según Hondius[80], quienes generaban los datos personales no podían conocer si éstos eran exactos y relevantes, y no había normas concretas sobre cómo almacenarlos y administrarlos adecuadamente.

[79] Adelantándonos a los capítulos posteriores, a los efectos del problema objeto de estudio en este trabajo, la Sentencia por el *Caso Digital Rights Ireland* -a la que haremos referencia en múltiples ocasiones, por cuanto fue la primera de una serie de sentencias que han cambiado el paradigma de la conservación de datos en el ámbito de la actuación de las autoridades policiales y penales- dictaminó que la Directiva europea de Conservación de Datos *"no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta. Por lo tanto, debe considerarse que esta Directiva constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario". Además, "los datos personales conservados con arreglo a la Directiva, a los que podían tener acceso las autoridades competentes, podrían permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones y los medios sociales que frecuentan". En consecuencia, la declaró "inválida", aunque " perseguía un fin legítimo, pero la injerencia en los derechos citados era grave y no se limitaba a lo estrictamente necesario"*.

[80] Frits Hondius fue subdirector de DDHH en el Consejo de Europa y redactor del primer instrumento de protección de datos internacionalmente vinculante: el Convenio sobre protección de datos del Consejo de Europa de 1981. Para profundizar, vid., Manual del Delegado de Protección de Datos,

El derecho a la privacidad o al respeto a la vida privada se consagró en tratados internacionales posteriores a la Segunda Guerra Mundial: el Convenio Internacional de Derechos Civiles y Políticos de la ONU (ICCPR) y el Convenio Europeo de Derechos Humanos[81], y pretendía proteger fundamentalmente contra injerencias en la vida privada de las personas por parte de los Estados, entre otras formas, mediante la interceptación de las comunicaciones. Sin embargo, no era un tratado vinculante. No obstante, el Tribunal Europeo de Derechos Humanos también ha interpretado este derecho en el sentido inverso, es decir, que el Estado proteja a los ciudadanos contra la interceptación de sus comunicaciones por otros particulares sin una base legal habilitante[82].

El diccionario de la lengua española define la intimidad, en su segunda acepción como: "*2. f. Zona espiritual íntima y reservada de una persona o de un grupo, especialmente la familia"*. Podemos considerarla, de acuerdo con Sobrino García (2019; 689)[83], como el espacio personal, como el límite entre lo público y lo privado, entre lo confidencial y lo que puede enseñarse. Hay consenso en el carácter universal de la preservación de la intimidad[84]. Por su parte, Ruiz Miguel (1995; 128)[85] concibe la intimidad en derecho como una manifestación jurídica de una necesidad inminentemente social, como un ámbito inaccesible y reservado a cada individuo frente a terceros. Se atribuye a la persona, al individuo, la propiedad de la información

---

guía para los delegados de protección de datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea, elaborado para el proyecto "T4DATA" financiado por la UE, en https://www.aepd.es/sites/default/files/2019-12/El%20Manual/%2del%20DPD%/20-%20KORFFGEORGES%20-%ESP.pdf, p. 14

[81] El artículo 12 de la Declaración Universal de Derechos Humanos de 1948, fue el instrumento base tanto para el ICCPR como para el CEDH, y recogió que: *"nadie será sometido a interferencia arbitraria en su privacidad, familia, domicilio o correspondencia… "*El ICCPR y el CEDH se redactaron en paralelo en 1949-50 (pero el CEDH, que se abrió a la firma a finales de 1950 y entró en vigor en 1953, entró en vigor más de veinte años antes del ICCPR, que se abrió a la firma en 1996 y entró en vigor en 1976).

[82] Vid., Sentencia de 25 de junio de 1997, ECtHR, Halford v. el Reino Unido.

[83] SOBRINO GARCÍA, I., *"Protección de datos y privacidad. Estudio comparado del concepto y su desarrollo entre la Unión Europea y Estados Unidos"*, UNED, Revista de Derecho, núm. 25, 2019, pp. 687-713, p. 689.

[84] Vid. PERRY, A., RUBINSTEN, O., PELED, L. y SHAMAY-TSOORY, S. *"Don't stand so close to me: A behavioral and ERP study of preferred interpersonal distance"*, Neuroimage, 83, 2013, pp. 761-769.

[85] RUIZ MIGUEL, C., *La configuración constitucional del derecho a la intimidad*, Tecnos, Madrid, 1995, p. 128

personal, que conforma su personalidad y desarrollo y, en consecuencia, se le otorga el derecho de decidir a quien la comunica y con quien la comparte. Y ciertas características concretas de esa intimidad: como la religión, las creencias políticas, la orientación sexual, etcétera, requieren de especial protección ante injerencias externas. En definitiva, es un concepto vinculado al de la dignidad personal y de libertad individual. Privacidad e intimidad no son sinónimos; normalmente, a los asuntos relacionados con la intimidad (sentimientos, pensamientos e inclinaciones más internos) se les denomina en plural, *"intimidades"*[86].

Este derecho, según Sobrino García (2019; 690)[87], no se configuró como tal hasta finales del siglo XIX, reconociéndose anteriormente ciertos aspectos de él, pero no como una concepción global. Y es precisamente debido a intromisiones de la prensa en el ámbito personal y familiar, cuando se inicia esa andadura. A partir de ese momento, como relatan Brandeis y Warren[88] se concibe como "*the right to be alone"*, y es reconocido por los tribunales americanos y posteriormente por la Declaración Universal de Derechos Humanos. Martínez de Pisón (2016; 412)[89] argumenta que se trataba de proteger el espacio íntimo de la intromisión o injerencia de terceros; en definitiva, como la ausencia de coacciones externas que dificulten las decisiones o acciones de una persona.

Así las cosas, como indicábamos antes, en Europa se recogió en el Convenio Europeo de Derechos Humanos de 1950, de forma concreta en su artículo 8:

1. *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y correspondencia.*
2. *No podrá haber injerencia de la autoridad [pública] en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria*

[86] Vid. CONDE ORTIZ, C., *La protección de datos personales un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid, Dykinson, 2005.

[87] SOBRINO GARCÍA, I.*," Protección de datos y privacidad…",* op. cit. p. 690.

[88] Vid. BRANDEIS, L.D y WARREN, S.D, *"The right of …",* op. cit. p. 1

[89] MARTÍNEZ DE PISÓN, J., *"El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional",* Anuario de Filosofía del Derecho, núm. 32, 2016, pp. 409-430, p. 412.

para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

Esta definición, que se ha configurado como uno de los ejes definidores del desarrollo y la protección de los derechos humanos y las libertades públicas, será muy tenida en cuenta por el TJUE a la hora de dictar las sucesivas sentencias que veremos más adelante.

No obstante, aunque este artículo del CEDH se ha aplicado de forma recurrente para dar protección a los individuos en relación a sus datos personales y a la recopilación, uso y conservación de estos, especialmente por las agencias encargadas de la aplicación de la ley[90], según Korff y Georges[91], en los años 70 y 80 del siglo pasado, la medida en que se podía confiar en el derecho a la vida privada en las relaciones entre individuos, y entre estos y las entidades privadas todavía no estaba muy claro. En cualquier caso, los individuos no pueden iniciar en base al CEDH -o el ICCPR[92]- una acción contra otros particulares, sino como máximo iniciar acciones contra el Estado correspondiente por no protegerles.

Es cierto que estamos usando de forma casi indistinta los conceptos de intimidad, privacidad, y de forma muy parecida el de protección de los datos personales, lo que pudiera dar a entender que son casi idénticos. No obstante, si bien pudiera ser así al principio, con el paso del tiempo el significado de cada uno de ellos se ha ido determinando de una forma más concreta. No obstante, a los efectos de este estudio, no parece relevante profundizar en exceso en esta cuestión. Veremos que el propio

[90] Factsheet -Personal Data Protection, 2018, del Consejo de Europa, disponible en: https://www.coe.int/en/web/data-protection/echr-case-law.

[91] KORFF, D., y GEORGES, M., "*Guía para delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea"*, 2019, p. 11.

[92] El Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés), fue adoptado por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966 y entró en vigor el 23 de marzo de 1976. El pacto desarrolla los derechos civiles y políticos y las libertades recogidas en la Declaración Universal de los Derechos Humanos. Para ampliar, vid. https://www.coe.int/es/web/compass/the-international-covenant-on-civil-and-political-rights

Tribunal de Justicia de la Unión Europea los usa en ocasiones también de forma casi indistinta en las sentencias que analizaremos. En común acuerdo con Sobrino García (2019; 692)[93], consideramos que todos ellos contienen un elemento característico y distintivo coincidente, en cuanto que representan la idea de la existencia de una esfera privada en la que cada persona tiene la facultad y la potestad de decidir lo que le afecta y autorizar o prohibir intromisiones no deseadas. Actualmente, algunos autores abogan por que, en momentos en los que se está extendiendo lo que Fernández Barbudo (2019; 71 y ss.) [94], llama *"el desarrollo de la economía de la vigilancia"* de carácter económico, se atienda a la necesidad de una perspectiva colectiva de la privacidad, a la existencia de una dimensión colectiva sobre la privacidad que trasciende el ámbito individual de decisión, que no se centre exclusivamente en el individuo.

2. La vida privada y su configuración en la Unión Europea

La vida privada, la intimidad, la vida íntima se concibe como una libertad, la libertad de impedir o limitar el acceso de otros a un ámbito personal, a impedir o limitar la injerencia externa a una parte privada de la persona. El Tribunal Europeo de Derechos Humanos, en su sentencia de 16 de diciembre de 1992, en el caso *Nimietz c. Alemania*, consideró como restrictivo el reducir el ámbito al círculo interior en el que el individuo desarrolla su propia vida personal[95]. En ese sentido, la vida privada debe englobar hasta cierto punto el derecho a establecer y desarrollar relaciones con otras personas, agrupando acciones tan variadas como las relativas a la vida e identidad sexual, los datos de la salud, o incluso la elección del propio nombre. En definitiva, argumenta Sobrino García (2019; 693)[96], *"se busca reconocer al individuo unos derechos que le corresponden por el hecho de ser persona, de tal forma que la persona no tiene que ejercitar acción alguna, ni cumplir otros requisitos que el mero hecho de serlo"*.

[93] SOBRINO GARCÍA, I., *"Protección de datos y privacidad…"*, op. cit. p. 692.

[94] FERNÁNDEZ BARBUDO, C., *"Hacia una privacidad colectiva: repensar las bases teóricas de la distinción público/privado en la economía de la vigilancia"*, Teknokultura, Revista de Cultura Digital y Movimientos Sociales, Ediciones Complutense, 2019, pp. 69-76, p. 75

[95] Sentencia del TEDH, de 16 de diciembre de 1992, Caso Niemietz contra Alemania, art. 6.1, Derecho al proceso justo; acceso al tribunal en https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001-164616&filename=CASE%20OF%NIEMEIETZ%20V.%20GERMANY%20-%20%5BSpanish%20Translation%5D%20summary%20by%20the%20Spanish%20Corte%20Generales.pdf&logEvent=False consultada el 27 de agosto de 2022.

[96] SOBRINO GARCÍA, I., *"Protección de datos y privacidad…"*, op. cit. p. 693.

El TJUE también ha abordado esta cuestión y reconoce a este derecho como fundamental y protegido por el ordenamiento jurídico comunitario. Considera que el respeto a la vida se encuentra consagrado en el CEDH como uno de los derechos fundamentales. Además, como asevera Tejerina Rodríguez (2014; 231)[97], el respeto a la vida privada exige el respeto también de la negativa de su titular a que sea conocida en toda su extensión.

Empero, como decíamos en párrafos precedentes, se reconoce también que ningún derecho es absoluto y, en consecuencia, se establecen límites a su ejercicio. En ese sentido, la sentencia del TEDH de 24 de febrero de 1998, *Caso Botta c. Italia*[98] ha establecido que debe ser entendido como derecho a la intimidad siempre que se muestre la existencia de un vínculo directo entre las medidas buscadas por el demandante y su vida privada y familiar. Por su parte, la propia redacción del artículo 8.1 del CEDH recoge claramente los aspectos a los que afecta esa protección y los límites que se puedan establecer, siempre que estén previstos en la ley y sean necesarios para, entre otros supuestos, la seguridad nacional y la seguridad pública.

Respecto de la privacidad, no solo hace referencia a la intimidad, sino que se extiende también al ámbito familiar de la persona, a sus aficiones, a sus bienes particulares y a sus actividades personales. El diccionario de la Real Academia Española la define como: *"2. Parte más interior o profunda de la vida de una persona, que comprende sus sentimientos, vida familiar o relaciones de amistad"*. En ese sentido, Rebollo Delgado (2008; 41)[99] observa que la vida privada está configurada en función de un ámbito interior, que afecta a la moralidad y el pensamiento del individuo; y otro externo, en el que se toma referencia respecto de los demás. Y, en consecuencia, engloba todos aquellos datos relativos a la persona, su domicilio, sus comunicaciones y

[97] TEJERINA RODRÍGUEZ, O., *Seguridad del Estado y privacidad*, Edición Reus, 2014, p.231

[98] Vid. Sentencia Caso Botta contra Italia, dictada en Estrasburgo el 24 de febrero de 1998 en el caso Botta contra Italia, el Tribunal europeo declara, por unanimidad, que los artículos 8 y 14 del Convenio Europeo de Derechos Humanos no son aplicables.

[99] REBOLLO DELGADO, L., "*Vida privada y protección de dato…"s*, op. cit. p. 41.

sus relaciones personales y afectivas, de forma que la persona tiene derecho a su control en cualquiera de estos casos.

3. El derecho a la protección de los datos de carácter personal

Como muchos de los otrora adelantos que hoy usamos de forma cotidiana por el público general, los ordenadores se construyeron por primera vez con fines militares, en la Segunda Guerra Mundial. La necesidad de proteger los derechos y las libertades en relación con el tratamiento automatizado de datos personales surge más tarde, en la década de 1960, cuando los ordenadores comenzaron a utilizarse de forma generalizada tanto en el sector público como privado. A finales de esa década y principios de los 70 comenzaron los debates en ese sentido en Alemania, Noruega, Suecia, Francia, Reino Unido, EE. UU., y otros países, así como en la OCDE[100] y el Consejo de Europa[101]. Estos primeros debates, según indican Korff y Georges (2019; 12)[102], tuvieron lugar entre profesionales sujetos a obligaciones éticas y entre políticos que estaban preocupados por los riesgos por abuso o uso indebido o seguridad de los datos personales tratados de manera automática.

A principios de los 80 del siglo pasado estos se extendieron a poblaciones más amplias, bien por las acciones gubernamentales tendentes a crear bases de datos nacionales sobre aspectos de la intimidad de los ciudadanos, como en Francia, o por el miedo a violaciones de la privacidad que ofrecía el uso de las nuevas tecnologías, así como por las posibles consecuencias de los errores de los datos almacenados y tratados, como en Alemania. Esta situación propició la demanda respecto del respaldo legal a la protección de los datos personales. Con el paso del tiempo, los tribunales

[100] La Organización para la Cooperación y el Desarrollo Económicos (OCDE) es una organización internacional cuya misión es diseñar mejores políticas para una vida mejor, fundada en 1961 y compuestas por 38 estados. En colaboración con los gobiernos, responsables de políticas públicas y ciudadanos, trabaja para establecer estándares internacionales y proponer soluciones basadas en datos empíricos a diversos retos sociales, económicos y medioambientales. Para profundizar, vid. https://www.oecd.org/acerca

[101] El Consejo de Europa aprobó las primeras resoluciones del consejo de ministros en 1973 y 1974. Vid. Memorándum Explicativo al Convenio Europeo de Protección de Datos, disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000016800ca434

[102] KORFF, D., y GEORGES, M., *"Guía para delegados de Protección de Datos…"*, op. cit., p. 12.

constitucionales y otros tribunales superiores fueron dictando sentencias avalando esa demanda y se adoptaron también instrumentos jurídicos internacionales.

El término *protección de datos* proviene del término alemán *Datenschutz*, y se utilizó por primera vez en la Ley de protección de datos de 1970 (Datenschutzgesetz) del Estado alemán de Hesse, redactada por el que ha sido considerado como el padre de la protección de datos, el Profesor Spiros Simitis[103]. Indican Korff y Georges (2019; 12), citando a Burkert [104], que el título era inapropiado, puesto que la *"la ley no protegía los datos, sino los derechos de las personas cuyos datos se estaban manejando"*. Hoy se ha extendido el término protección de datos, como abreviatura de *"la protección de los individuos con respecto al tratamiento de datos personales*".

El derecho a la protección de los datos, como decíamos, viene asociado al desarrollo de las nuevas tecnologías y su relación con la intimidad, que han propiciado una mayor atención hacia el valor de los datos personales. Asevera Ballesteros Moffa (2018; 50)[105] que este derecho ha tenido que ir adaptándose para cubrir los distintos flancos que la sociedad tecnológica ha ido creando, siempre detrás de esos avances, que ha ido generando diversos riesgos, pero con un denominador común: resultar *"invisibles para su titular"*. Actualmente, se habla de este concepto con gran familiaridad y cotidianidad entre personas de diferentes generaciones: el concepto de los datos personales[106] y su valor. Además, el debate ha girado hacia la desconfianza, -queremos decir- hacia el pensamiento de que el uso que empresas y particulares hacen de los datos

[103] Hessisches Datenschutzgesetz (Ley de Protección de Datos del Land de Hesse) 1970, en vigor desde el 13 de octubre de 1970, B.O.E del Land, Parte I, 1970, Nr. 41 (12 de octubre de 1970), disponible en: https://starweb.Hesse.de/cache/GVBL/1970/00041.pdf

[104] Cfr. HERBERT BURKERT, Privacy-Data Protection: *"A German/European Perspective"* (Protección de la Privacidad de los Datos) (sin fecha), p. 46, disponible en: http://www.coll.mpg.de/sites/www/files/text/brukert.pdf

[105] BALLESTEROS MOFFA, L.A., *"La revisión del régimen jurídico de la privacidad en la Unión Europea",* Revista del posgrado en Derecho de la UNAM, Nueva Época, nº. 8, enero-junio 2018, pp. 40-68, p. 50.

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

personales que los ciudadanos proporcionamos, se dirige normalmente en sentido opuesto al respeto de los derechos básicos de las personas.

El derecho a la protección de los datos personales surgió entonces como respuesta a esa desconfianza generada por la rápida evolución de la sociedad de la información, y emergieron posturas enfrentadas sobre el reconocimiento de un nuevo derecho frente a la restructuración del derecho a la intimidad[107]. En consecuencia, esa protección se produjo por la evolución tecnológica que hizo evidente la necesidad de protecciones adicionales para los individuos. Por ello, en la Unión Europea el derecho a la protección de datos lleva asociado también la necesidad de consentimiento expreso del titular de los datos, que decide en cada caso en qué circunstancias permite su uso y tratamiento, salvo que la ley establezca otra cosa distinta. Esta concepción se ha ido desarrollando a lo largo del tiempo y nos referiremos a ella a continuación. Fuere como fuere, según Korff y Georges (2019; 14)[108] todos los Estados europeos coinciden con Hondius en lo que ya expuso en 1983 al respecto de que *"la protección de datos tiene como objetivo salvaguardar un equilibrio justo y razonable entre los intereses de los individuos y los de la comunidad a la que pertenecen"*. Ahora bien, alcanzar ese equilibro es una de las cuestiones fundamentales y, al mismo tiempo, más complejas, por lo que le dedicaremos atención especial en capítulo aparte, por cuanto supone uno de los elementos fundamentales que provocaron la invalidación de la Directiva europea de 2006 sobre conservación de datos y que ha motivado una situación que se alarga demasiado en el tiempo y ha dado origen a este estudio. Ahora, solo a modo de pincelada, siguiendo el criterio expuesto por Korff y Georges en la citada guía para delegados de protección de datos[109], esbozamos algunas de las características que recogen los principios reguladores que permiten alcanzar el equilibrio necesario:

- *"La recopilación y posterior uso y divulgación de datos personales deben estar sujetos a la ley* [es decir, a las normas jurídicas vinculantes, en lugar de códigos voluntarios o directrices no vinculantes]*;*

[107] Cfr. ORTÍ VALLEJO, A. *"Derecho a la intimidad e informática, Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada"*, Comares, Granada, 1994.

[108] KORFF, D., y GEORGES, M., *"Guía para delegados de Protección de Datos…,"*,op. cit. 14

[109] *Ibíd.*

- *Deben ser leyes generales* [ómnibus] *que, en principio, se aplican a todas las entidades públicas y privadas que procesan datos personales -con excepciones y modificaciones de las reglas y principios previstos en normas especiales cuando sea necesario, pero siempre respetando su 'núcleo esencial';*
- *Deben contener ciertas normas sustantivas básicas y otorgar a los interesados derechos humanos fundamentales; y*
- *Su aplicación debe ser supervisada por órganos especiales de supervisión -generalmente denominadas agencias de protección de datos o APD-".*

A la ley del Estado alemán de Hesse siguieron otras también nacionales en Suecia, Francia, Austria, Dinamarca y Noruega, que se unieron en torno a un conjunto de principios y derechos fundamentales que fueron progresivamente aceptados y tenidos en cuenta por otros instrumentos no vinculantes del Consejo de Europa[110].

Esos mismos principios se extendieron más tarde a nivel mundial, igualmente de forma no vinculante, a otros instrumentos como: las Directrices de la OCDE de 1980 sobre la Protección de la privacidad y los flujos transfronterizos de datos personales[111] y las Directrices de las Naciones Unidas de 1989 para la regulación de los archivos informatizados de datos personales[112]. Este último reconoce por primera vez la importancia de contar con agencias independientes que garanticen la protección de los datos personales.

[110] Resolución del Consejo de Europa de 1973 (73)22 sobre Protección de la privacidad de las personas frente a los bancos electrónicos en el sector privado, en https://rm.coe.int/CoERMPbulicCommonSearchServices/DisplayDCTMContent?documentId=090000168 0502830

Resolución del Consejo de Europa 1974 (74)29 sobre Protección de la privacidad de las personas frente a los bancos de datos electrónicos en el sector público, en https://www.oecd.org/sti/iconomy/oecdguidelinesonttheprotectionofprivacyandtransborderflowsofpersona l_data.htm

[111] OCDE, Recomendaciones del Consejo acerca de las Guías que rigen la Protección de la Privacidad y el flujo transfronterizo de datos personales, de 23 de septiembre de 1989, en: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtrnasborderflowofpersona l_data.htm

[112] Naciones Unidas, Guía para la regulación de los ficheros automatizados de datos personales, UNGA Res. 44/132, 44 UN GAOR Supp. (Nº. 49) en 211, UN Doc. A/44/49 (1989), en https://www1.umn.edu/humanrts/instree/q2grcpd.htm

3.1 Convenio núm. 108 del Consejo de Europa y su Protocolo Adicional

El Convenio 108, del 1981, del Consejo de Europa[113] constituye el marco genérico que protege a la persona frente a abusos a su intimidad. Aunque es una organización de la que forman parte también Estados no europeos[114], todos los Estados miembros de la Unión Europea lo han ratificado[115]; incluso la propia Unión Europea como tal, representada por la Comisión, es miembro también del Consejo de Europa[116]. Su valor fundamental radica en que se convirtió en el primer instrumento jurídicamente vinculante en el ámbito internacional en materia de protección de datos; un instrumento relativamente reciente. En 2001, el Convenio fue complementado por un Protocolo Adicional[117]. Posteriormente, incluyó un artículo específico para regular el tratamiento de categorías especiales de datos que, si bien se refieren a unos datos concretos que no afectan al objeto de este estudio, sí nos sirve a los efectos de poner de manifiesto que existen diferentes tipos de datos sobre los que se despliegan diferentes garantías. Esto no es relevante en este momento, pero sí será abordado más adelante, cuando estudiemos las diferentes categorías de datos que se puedan establecer respecto de la conservación de metadatos generados por las comunicaciones electrónicas. Como anécdota, pero ilustrativa de que no era una discusión pacífica, exponen Korff y Georges[118] (2019; 18) que en los debates durante la negociación de este instrumento normativo: *"la necesidad de reglas especiales sobre ciertos tipos de datos se debatió acaloradamente en su momento.* Algunos de los ponentes defendieron la sensibilidad de cualquier tipo de dato, en función de las circunstancias concretas; mientras que otros abogaron por que se algunos de los que se pretendía incluir bajo esa categoría, podían no serlo si se tenían en cuenta esas circunstancias concretas. Finalmente, se aprobó la

[113] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. El protocolo de modificación del Convenio 108 fue adoptado por el Comité de ministros del CE el 18 de abril de 2018 (CETS nº. 223).

[114] El artículo 23 prevé que pueda ser ratificado por otros Estados no miembros, si son invitados a ello.

[115] Hasta ahora ha sido ratificado por 55 estados: Uruguay, 2013; Mauricio, 2016; Senegal, 2016; Túnez, 2017; Cabo Verde y México, 2018. Y han sido invitados Argentina y Burkina Faso.

[116] En 1999 se modificó la propia base reguladora del CdE en ese sentido.

[117] *"Consejo de Europa, Protocolo Adicional al Convenio para la protección de las personas con respecto al procesado automático de datos personales en relación con las autoridades de supervisión y los flujos de datos transfronterizos"*, abierto para su firma en Estrasburgo el 8 de noviembre de 2001, CETS, en: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000001680080626 Ha sido ratificado por 36 de los 47 estados miembros y por los 6 seis que no son miembros. Además, se ha invitado a Burkina Faso.

[118] KORFF, D., y GEORGES, M., *"Guía para delegados de Protección de Datos…"*, op. cit., 18.

propuesta del representante francés Louis Joinet[119], a la sazón también presidente del comité responsable de la elaboración y se consideró que todos los datos debían ser regulados, adjudicando una mayor protección a los *confidenciales o especialmente sensibles*.

Una cuestión importante del Convenio, y relevante también para esta tesis, es que permitió a los Estados firmantes la adopción de excepciones y restricciones a determinados requisitos de para, según el artículo 9 (2)[120], entre otras finalidades: proteger la *"seguridad del estado, la seguridad pública, [….] o la supresión de los delitos" o "los derechos y libertades de los demás", siempre que la excepción esté "prevista por la legislación del Estado-parte y constituya una medida necesaria [y proporcionada] en una sociedad democrática"* (Convenio 108; 36001).

En 2018, el Convenio fue actualizado para alinearlo con la legislación de la Unión Europea más reciente y las tendencias más actuales a nivel global de la protección de datos[121].

3.2 La legislación en Europa en materia de protección de datos

El Convenio 108, si bien estableció una serie de principios que permanecen vigentes hoy día, según el parecer de Sobrino García (2019; 697)[122] fue decayendo en eficacia al resultar incapaz de resolver problemas respecto de la transmisión fronteriza de datos, principalmente por el escaso número de países ajenos a la Unión Europea que lo subscribieron o porque no todos los firmantes lo incorporaron a su legislación nacional. Por consiguiente, la Unión Europea, cuyos Estados miembros constituían el grueso de países firmantes y, como contraposición al objetivo de ese momento de avanzar hacia la armonización de las normas que permitieran un mercado interior

[119] Louis Joinet fue un juez francés, representante en el Comité de Derechos Humanos de las Naciones Unidas que se encargó de redactar las Guías de las Naciones Unidas.

[120] Artículo 9.2 del Convenio 108, relativo a la excepción y restricciones: *"Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática"* en https://www.boe.es/boe/dias/1985/11/15/pdfs/A36000-36004.pdf

[121] Para profundizar, vid. https://www.coe.int/es/web/data-protection/convention108/modernised.

[122] SOBRINO GARCÍA, I., *"Protección de datos y privacidad…"*, op. cit. p. 697.

europeo, emprendió el camino hacia la armonización también de las normas que operaban en el sector de las telecomunicaciones. Esto dio lugar al punto de partida hacia leyes de protección fuertes y de general aplicación en los Estados miembros.

El resultado práctico de ese cambio de rumbo se tradujo en una propuesta de la Comisión Europea de un conjunto de normas destinadas a la protección de los datos del *"primer Pilar"* de la Comunidad Europea[123]:

- Una norma referida a la protección de las personas en relación con el tratamiento de sus datos personales, que se convirtió en la principal Directiva en la materia: la Directiva 95/46/CE, y
- Una Directiva sobre la protección de los datos personales en el contexto de las redes públicas de telecomunicaciones digitales y las redes móviles digitales públicas, que dio lugar a la Directiva 97/66/CE de protección de datos de telecomunicaciones, reemplazada en 2002 por la Directiva 2002/58/CE, que se conoce como Directiva de privacidad electrónica.

Han pasado ya veintisiete años desde la aprobación de la Directiva 95/46/CE y ha permanecido vigente hasta hace pocos años. Se puede considerar como la primera norma propia de la Unión Europea que establece el sistema de protección de las libertades y de los derechos fundamentales de los europeos y, de forma particular de su intimidad, respecto del tratamiento de sus datos personales. Como directiva que es, se proponía armonizar y aproximar las disposiciones de los Estados miembros, pero al mismo tiempo, establecer un equilibrio entre un nivel elevado de protección de la vida privada y la libre circulación de datos personales dentro de la Unión y, en ese sentido, fijaba límites estrictos para la recogida y utilización de los datos personales, además del establecimiento de un organismo independiente en cada Estado miembro encargado de

[123] El Tratado de la Unión Europea, firmado en Maastricht el 7 de febrero de 1992 (conocido como el "Tratado de Maastricht"), preveía una estructura de tres pilares. El primer pilar estaba formado por la Comunidad Económica Europea (CEE), la Comunidad Europea del Carbón y del Acero (CECA) y la Comunidad Europea de la Energía Atómica (CEEA) y posteriormente abarcaba el mercado único creado en 1993. Los pilares segundo y tercero abarcaban, respectivamente, la Política Exterior y de Seguridad Común (PESC) y la cooperación en los ámbitos de la Justicia y Asuntos de Interior (JAI). Los pilares fueron formalmente *"demolidos"* por el Tratado de Lisboa, aunque no ha desaparecido la aprobación de instrumentos de forma separada según las áreas que esos pilares abarcaban.

la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales.

Respecto de los límites al derecho a la protección de los datos, la aplicación de esta Directiva ha sido sometida también al TJUE, que se ha pronunciado en varias ocasiones. Tomaremos aquí dos sentencias concretas en las que se aportan reflexiones interesantes al objeto del presente estudio:

- En primer lugar, en relación con el derecho a la libertad de expresión, como recoge Piñar Mañas (2003; 47) [124] en la sentencia al *Caso Bodil Lind-qvist c. Göta hovrätt (Suecia)*, de 6 de noviembre de 2003, en la que *colisionan* el derecho a la protección de datos personales tan sensibles como los relativos a la salud, y la libertad de expresión. El Tribunal entendió que para ponderar los distintos derechos e intereses existen disposiciones en la Directiva 95/46/CE que deben tenerse en cuenta junto a las disposiciones nacionales. Así pues, para alcanzar un equilibrio justo entre ambos derechos se debe acudir a las normas nacionales pertinentes al caso concreto, puesto que las disposiciones de la Directiva son muy generales y corresponden a un número diverso de situaciones diferentes.

- En segundo lugar, el tratamiento de datos personales exige una base legal que lo habilite y, en ausencia de ella, constituiría una violación de tal derecho. Además, los datos objeto de tratamiento no tienen por qué ser confidenciales o potencialmente causantes de un daño al individuo para que deban ser protegidos. Dos sentencias del TJUE avalan esta afirmación: el *Caso Google España*[125] de 13 de mayo de 2014 -que dio un respaldo al llamado *"derecho al olvido"*[126]-, en la que el Tribunal sentenció que el procesamiento de los datos personales representa una amenaza al propietario de los datos y solo se puede llevar a cabo si una ley lo permite y determina la

[124] PIÑAR MAÑAS, J.L. *"El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas"*, Cuadernos de Derecho Público, 19, 2003, pp. 45-90.

[125] Vid. Sentencia del Tribunal de Justicia (Gran Sala), de 13 de mayo de 2014, en el asunto C-131/12.

[126] Grosso modo, se trata de la posibilidad de un ciudadano de borrar sus datos personales y su *"rastro"* en la red.

forma en que se materializa; otra, la *Sentencia de 6 de octubre de 2015 Schrems*[127], en la que el Tribunal determina que no es necesario que la información tratada sea sensible o haya producido alguna consecuencia adversa sobre el titular de los datos para que se considere una injerencia en el derecho fundamental al respeto a la vida privada. Analiza Minero Alejandre (2017; 53)[128] la primera de las sentencias citadas y arguye que el *"TJUE no crea un derecho nuevo [el derecho al olvido]… sino que lo pionero del pronunciamiento es la identidad del sujeto contra el que se dirige la reclamación para el ejercicio del derecho al olvido"*.

A través de esta norma se creaban también dos organismos europeos que llevan el nombre de los artículos bajo los que fueron creados y que han sido muy relevantes en el devenir de los tiempos en esta materia:

- El denominado *"Grupo de trabajo del artículo 29 (GT29; o WP29, por sus siglas en inglés)*[129]*"*, constituido como un organismo independiente y compuesto por representantes de las autoridades de protección de datos de los Estados miembros, así como del Supervisor Europeo de Protección de Datos (SEPD)[130] y un representante de la Comisión Europea. Desde su constitución han sido muchos los documentos y opiniones que han generado, no solo con la Directiva 95/46/CE, sino también sobre la interpretación de la Directiva de privacidad electrónica, que lo posiciona como una fuente de consulta muy importante, ya que, aunque sus dictámenes no son vinculantes, la autoridad que ha ejercido los hace casi *de obligada consideración.*

[127] Sentencia del Tribunal de Justicia (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14.

[128] MINERO ALEJANDRE, G., "*Presente y futuro de la protección de datos personales*. *Análisis normativo y jurisprudencial desde una perspectiva nacional y europea"*, Anuario Jurídico y Económico Escurialense, 2017, pp. 13-58, p. 53.

[129] El sucesor de este Grupo es el Comité de protección de datos, que empezó sus trabajos el 25 de mayo de 2018.

[130] El Supervisor Europeo de Protección de Datos (SEPD; o EDPS, por sus siglas en inglés) tiene la función de garantizar que, a la hora de tratar datos personales, las instituciones y organismos de la UE respeten el derecho a la intimidad de los ciudadanos. Se creó en 2004. Para profundizar, vid. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/edps_es.

- El conocido como *"Comité del artículo 31"*, compuesto por representantes de los Estados miembros y presidido por un miembro de la Comisión. Emite dictámenes sobre los proyectos de medidas a adoptar.

Por su parte, la Directiva de protección de datos de telecomunicaciones, se aprobó el 15 de diciembre de 1997[131]. Esta Directiva es considerada como una ley especial en relación con la Directiva 95/46/CE. Poco después, en 1999, se revisó el marco regulador de las comunicaciones electrónicas y se presentó una nueva propuesta legislativa que culminó con la adopción, en julio de 2002, de la Directiva 2002/58/CE de privacidad electrónica[132]. También es considerada como una ley especial de la Directiva del 95.

Esta Directiva trajo consigo una serie de normas relativas al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Su objetivo principal era eliminar el envío masivo de correos electrónicos y, para ello, se establecieron una serie de reglas que garantizasen la seguridad y confidencialidad de las comunicaciones en redes de internet y servicios móviles de la Unión Europea. El interés de esta norma radicaba, por un lado, en la regulación de la confidencialidad de las comunicaciones, al establecer que los Estados miembros tenían que garantizar mediante su legislación la confidencialidad de las comunicaciones y de los datos de tráfico, y se prohibía la escucha, la grabación, el almacenamiento u otro tipo de intervención o vigilancia de las comunicaciones y de los datos de tráfico asociados a ellas por personas distintas a los usuarios, sin el consentimiento de los mismos, salvo que estuvieran autorizadas [legalmente] para hacerlo.

[131] Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, OJ L24, 30.01.1998, pp. 1-8, en: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN

[132] 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), OJ L201, 31.07.2002, pp. 37 – 47, en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

Posteriormente, en 2009, la Directiva del 2002 se modificó de nuevo mediante la Directiva 2009/136/CE[133]. Actualmente, tras varios años de avances y paradas[134], sigue en periodo de negociación entre los colegisladores[135] una nueva norma de protección de la privacidad electrónica, esta vez en forma de reglamento.

Esta Directiva tiene un ámbito de aplicación más limitado que la considerada como Directiva general, pues se refiere solo a los datos personales en relación con *"la prestación de servicios de comunicaciones electrónicas accesibles para el público en redes de comunicación públicas"*. No entraremos ahora a definir los elementos relevantes que forman parte de este proceso, pues más adelante le dedicaremos un apartado específico, dada su importancia para el objeto de estudio.

Citaremos, eso sí, un artículo que fue tomado como cláusula habilitante para la aprobación de la Directiva de conservación de datos [posteriormente invalidada por el Tribunal de Justicia de la Unión Europea]. Nos referimos al apartado 1 del artículo 15 de la Directiva sobre privacidad electrónica, que habilita a los Estados miembros a poder restringir los derechos y las obligaciones recogidas por la Directiva [de privacidad electrónica] sobre la base de la cláusula de derogación de interés público de la Directiva principal [95/46/CE], es decir *"cuando dicha restricción constituya una medida necesaria, apropiada y proporcionada dentro de una sociedad democrática para salvaguardar la seguridad nacional, la defensa, seguridad pública y la prevención, investigación, detección y enjuiciamiento de delitos"* (Directiva 2002/58/CE, 2002; L201/46) . De esa forma, los Estados miembros podrán, entre otras cosas, adoptar medidas legislativas que prevean la conservación de datos durante un periodo de tiempo

[133] Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº. 2006/2004 sobre la cooperación en materia de protección de los consumidores, OJ L337, 18.12.2009, pp. 11-36, en https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:ES:PDF

[134] Algunas presidencias de turno del Consejo de la Unión Europea, conscientes de las dificultades para avanzar en el expediente, lo dejaban aparcado, con diferentes argumentos que, a nuestro modo de ver, intentaban ocultar el verdadero motivo: la falta de consenso para alcanzar un texto con mayoría suficiente.

[135] El Consejo de la UE y el Parlamento Europeo. En capítulo aparte se aborda la muchas veces difícil relación entre estas dos instituciones europeas con competencias compartidas en la producción normativa en determinadas materias.

limitado, de acuerdo con las excepciones que recoge el referido artículo de la Directiva de privacidad electrónica.

Respecto del Tercer Pilar[136], entre los años 1990 y 2009, la Unión Europea creó una serie de organismos/agencias y bases de datos y sistemas, además de normas y procedimientos para su uso y aplicación, con la finalidad de favorecer el intercambio de información entre autoridades policiales y judiciales de los Estados miembros. Aunque muchas de las normas que amparaban la adopción de estas medidas se inspiraron en la Directiva 95/46/CE y en el Convenio del Consejo de Europa, según Peter Hustinx[137]: *"el nivel de protección era más bajo en términos de alcance y sustancia"*[138] (Hustinx, 2014; 15). Con el Tratado de Lisboa y el fin de los pilares en la Unión Europea, se estableció un periodo transitorio para la adaptación del marco jurídico comunitario a la nueva realidad jurídica.

En el año 2000, con la CDFUE se reconoció de forma autónoma el derecho a la protección de los datos personales y esto ha producido efectos institucionales importantes que relata Rodotà (2006; 549)[139]: *"como las dos comunicaciones con las que la Comisión Europea ha establecido que sus actos legislativos y reglamentarios deben estar sometidos siempre a un control preliminar de compatibilidad con la Carta de los Derechos Fundamentales"*. Además, el ámbito de la protección de los datos personales ha dejado de estar vinculado al mercado interior, para pasar al ámbito del EJLS y, por tanto, no ligado exclusivamente a la lógica económica, puesto que afecta a personas más que objetos o mercancías.

[136] Dejaremos al margen las medidas del Segundo Pilar, por no ser relevantes a los efectos del presente estudio.

[137] Supervisor Europeo de Protección de Datos entre los años 2004 y 2014.

[138] PETER HUSTINX, *"EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation"*, pp. 1-52, p. 15, en: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

[139] RODOTÀ, S., *"La conservación de los datos de tráfico en las comunicaciones…"*, op. cit., p. 45.

3.2.1 Directiva 2006/24/CE de conservación de datos de las comunicaciones electrónicas

Esta Directiva es especialmente importante y nos referiremos a ella en numerosas ocasiones a lo largo del estudio -de hecho, ya lo hemos hechos de forma tangencial en pinas precedentes-. En este apartado, dedicaremos más tiempo y espacio a ella que para el resto de los instrumentos legislativos citados, precisamente por la razón antes apuntada.

Aunque la preocupación por garantizar los derechos y libertades de las personas en relación con los servicios propios de la Sociedad de la Información ha sido constante (de forma concreta a través de la protección de los datos personales), la lucha contra el terrorismo y otras amenazas a la Seguridad considera también esos servicios como un elemento fundamental al servicio de la prevención y de la investigación.

Como consecuencia de la necesidad de adoptar medidas para hacer frente a la amenaza terrorista que se cierne sobre Europa y, en concreto, tras los atentados de Madrid del 11 de marzo de 2004, se presentó una iniciativa de propuesta de Decisión Marco por Francia, Irlanda, Suecia y Reino Unido, con la idea de armonizar en los Estados miembros unas normas mínimas sobre la conservación de los datos de tráfico de comunicaciones[140] vista la importancia creciente que estos estaban adquiriendo en la investigación del terrorismo y otros delitos graves. Para ello, se propuso también la adaptación de la Directiva 2002/58/CE a esta nueva realidad generada por los ataques terroristas.

La base jurídica de la propuesta estaba basada en el Tercer Pilar, es decir, en el ámbito de la cooperación policial y judicial[141] y, respecto del procedimiento de aprobación, mediante unanimidad de los Estados miembros y sin informe vinculante del

[140] En aquel momento, los relativos a la fecha y hora de la comunicación, su origen y destino, etcétera.

[141] Se barajaron también otras opciones, aunque suelen ser las clásicas que la Comisión Europea maneja en sus evaluaciones de impacto ante cualquier propuesta normativa: no tomar ninguna medida, dejarlo abierto a la autorregulación por los Estados miembros o incluso adoptar una medida del Primer Pilar.

Parlamento Europeo. Esto provocó el rechazo de esta institución europea, que consideraba de gran importancia la materia, pero que solo ejercía un papel consultivo, no vinculante. Se produjo también la oposición del sector empresarial afectado y de diversas organizaciones sociales de defensa de los derechos civiles, que cuestionaban la proporcionalidad de las medidas, su eficacia y los costes que supondrían para las empresas afectadas, además de la vulneración de determinados derechos fundamentales, como la privacidad de los ciudadanos cuyos datos serían conservados por los operadores de telecomunicaciones. No tuvo éxito y finalmente no salió adelante la propuesta de decisión marco.

Los atentados de Londres del 7 de junio de 2005[142], en un momento en el que el Reino Unido ejercía la Presidencia de turno de la Unión Europea, añadieron presión sobre esta cuestión e hicieron que se retomara la necesidad de adoptar medidas; entre otras, en materia de conservación de datos de las comunicaciones electrónicas. Como resultado de ese nuevo impulso, se presentó otra propuesta, esta vez en forma de directiva, que resultó en la aprobación en el año 2006 de la Directiva 2006/24/CE[143], considerada una excepción a la norma general de protección de datos de 1995 y una aplicación excepcional a la Directiva de privacidad electrónica[144]. Establecía una obligación sobre los proveedores de servicios de telecomunicaciones de conservar los datos de tráfico y de localización, además de aquellos necesarios para la identificación del usuario o abonado y ponerlos a disposición de las autoridades competentes en determinados casos concretos y de acuerdo con un procedimiento establecido. Además de lo anterior, deberían conservar también los datos que permitieran identificar el destino de las comunicaciones y aquellos necesarios para identificar el equipo de comunicación de los usuarios: números de teléfono de origen y destino y el IMEI[145]. Se

[142] Así se reflejó en la Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo el 25 de marzo de 2004 (y contemplado en el Considerando 8 de la Directiva) y que surgió a raíz de que se le encargase al Consejo el examen de las medidas para establecer normas sobre la conservación de datos de tráfico de las comunicaciones por parte de los prestadores de servicios.

[143] Título completo: 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, OJ L 105, 13.4.2006, p. 54-63. Ver en http://data.europa.eu/eli/dir/2006/24/oj

[144] ORDOÑEZ SOLIS, D., *La protección judicial de los derechos en internet en la jurisprudencia europea*, Reus, Madrid, 2014.

[145] El término IMEI significa International Mobile Equipment Identity y es un identificador único que tiene cada teléfono móvil.

fijaba un periodo de conservación entre seis meses y dos años, y los sujetos obligados debían asegurar la calidad y seguridad de los datos retenidos y la transmisión de éstos sin demora.

La aprobación de la Directiva fue muy polémica, como hemos adelantado ya en los párrafos precedentes, y recibió numerosas críticas[146] del Grupo de trabajo del Artículo 29[147], aunque no solo: el Supervisor Europeo de Protección de Datos[148] y del Comité Económico y Social también fueron muy activos y beligerantes en su oposición a muchos de los preceptos del borrador. Fundamentalmente, se argumentaba que adolecía de falta de tutela adecuada de los derechos fundamentales afectados y [como veremos más adelante] fue precisamente la causa principal que motivó su invalidez por el Tribunal de Justicia europeo. También muchos autores escribieron mostrando sus dudas [o más bien certezas para ellos] respecto de las implicaciones de una norma como esta[149]. Por ejemplo, Rodotà (2006; 58)[150] afirmaba que *"no estamos discutiendo una directiva sectorial. Nos enfrentamos a una verdadera redistribución de poder social, una redefinición de la posición de la persona y de la ciudadanía"*. Creía el autor que la Directiva producía una modificación de los principios más básicos del derecho a la protección de los datos personales, hasta el punto de que provocaba un cambio más profundo que las producidas en momentos anteriores y produce *"un cambio en la manera de entender y regular la relación entre el ciudadano y el Estado, en la concepción misma de los derechos fundamentales de la persona. Así se reestructura no sólo el sistema jurídico sino también la organización social"*. (2006; 53 y 54) [151].

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

[147] Para profundizar sobre la creación, composición y cometidos del Grupo de trabajo del artículo 29, ver los artículos 29 y 30 de la Directiva 95/46/CE.

[148] El SEPD consideró que no se proporcionaba una respuesta proporcionada a las necesidades de la sociedad. Vid. Dictamen del SEPD, adoptado el 26 de septiembre de 2005 (2005/C 298/01), sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final], DO C 298 de 29.11.2005, p. 1, en: http://eur-lex.europa.eu/LexUriServ/site/es/oj/2005/c_298/c_29820051129es00010012.pdf

[149] Vid., VILASAU, M., "*La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad"*, IDP, Revista de Internet, Derecho y Política, núm. 3, UOC, pp. 1-15, p. 15.

[150] RODOTÀ, S., *"La conservación de los datos de tráfico en las comunicaciones…"*, op. cit., p. 58.

[151] *Ibíd*., pp. 53-54.

Volviendo al GT29, consideraba que estábamos ante una *"decisión histórica"*[152]. Al contrario de lo reflejado en el documento de evaluación de la Comisión Europea, que argumentaba que la conveniencia y la necesidad de la conservación de datos estaban suficientemente justificada, el GT29 creía que la necesidad debería apoyarse en pruebas y demostrarse claramente. De la misma forma, cuestiona también los períodos máximos de retención. En consecuencia, emitió en su dictamen -no vinculante- veinte garantías específicas, respecto de los requisitos aplicables a los destinatarios y al tratamiento de los datos, las autorizaciones y controles, las medidas a aplicar a los proveedores de servicios, las categorías de datos afectados y su actualización y la exclusión de los datos de contenido.

El Parlamento Europeo también aprobó una serie de enmiendas -en aquel momento tampoco eran vinculantes- hacia una mayor tutela de los derechos de los titulares de los datos. El Comité Económico y Social también se mostró preocupado por la redacción del borrador de Directiva y su inadecuado tratamiento del derecho a la privacidad y la desconfianza que esta situación generaría en los usuarios de los servicios de telecomunicaciones, además de los costes adicionales que la medida obligaría a soportar a los proveedores de servicios[153].

Otra cuestión relevante que también puso de manifiesto el Grupo del Artículo 29 era la falta de una definición clara sobre lo que se entiende por *delitos graves*, que también habremos de abordar más adelante. En ese sentido, propuso que los datos fueran conservados con la finalidad de luchar contra el terrorismo y la delincuencia organizada; es decir, de forma más precisa y acotada.

---

[152] Dictamen 4/2005, adoptado el 21 de octubre de 2005 (1868/05/ES. WP 113), sobre la Propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM (2005)438 final de 21.09.2005], en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_es.pdf

[153] Dictamen del Comité Económico y Social Europeo, de 19 de enero de 2006, sobre la "Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE" COM (2005) 438 final – 2005/0182 (COD). (2006/C 69/04). DO C 69 de 21.3.2006, p. 16., en http://eur-lex.europa.eu/LexUriServ/site/es/oj/2006/c_069/c_06920060321es00160021.pdf

Respecto del contenido de la Directiva, analizaremos solo determinadas cuestiones específicas, que nos ayudarán a comprender su devenir posterior ante el Tribunal de Luxemburgo:

- Las obligaciones que impone a los proveedores de servicios solo se circunscriben a los datos de tráfico y de localización, además de otros relacionados con el abonado o usuario (lo que se conoce como *metadatos*); es decir, queda excluido el contenido en sí mismo de las comunicaciones. Sobre esta parte, el propio grupo de trabajo se refiere a otros mecanismos de conservación y acceso a los datos con menor injerencia en los derechos de los afectados, como puede ser el *"quick freeze"*[154]que, grosso modo, prevé la conservación a partir de un determinado momento en que se obtiene una orden judicial para ello. Esta forma de conservación viene ya recogida en el Convenio de Budapest de 200, del Consejo de Europa[155]. No obstante, vemos claramente que excluye una cantidad importante de datos -en ocasiones, creemos que pueden ser fundamentales para determinadas investigaciones concretas- que se han generado antes del momento en que llega a conocimiento de los servicios policiales o judiciales los hechos sobre los que se pretende investigar.

- Sobre el término *"autoridades nacionales competentes"* como aquellas que puedan ser destinatarias de los datos conservados, según el Grupo del Artículo 29, ofrecía escasa precisión y pedía la publicación de un listado completo sobre quiénes cumplían con ese criterio. No podemos estar de acuerdo con esta apreciación -no se tuvo en cuenta- por cuanto sería más adecuado que las normativas nacionales de transposición fijaran esos límites. La publicación de un listado en la propia Directiva ofrecería cierta rigidez

[154] El Grupo del Artículo 29 menciona esta opción en el WP 113, p. 7. A modo de resumen, en este momento, el sistema de congelación rápida consiste en que la autoridad judicial o administrativa con competencia para ello, a requerimiento de los servicios policiales en el marco de una investigación concreta, oficie a los proveedores de servicios para que, desde ese momento, se conserven ciertos datos sobre una o más personas. Posteriormente, se autorizará a acceder a ellos o no, en función de criterios de necesidad y proporcionalidad. En el caso de no reunir elementos suficientes para que la autoridad correspondiente autorice el acceso y tratamiento, estos serán borrados.

[155] Convenio sobre la ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Para profundizar, vid. https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

ante futuros cambios en la denominación de los distintos cuerpos y organismos que conforman el conjunto de autoridades nacionales, que tendrían que ir incorporándose o saliendo de la lista en función de circunstancias variadas -alguna de las cuales ocurre con cierta frecuencia- como es el cambio de nombre o denominación y un cuerpo policial.

- En el artículo 5 de la Directiva, se especifican los datos concretos que serían objeto de conservación: *"los datos necesarios para i) rastrear e identificar el origen de una comunicación; ii) identificar el destino de una comunicación; iii) identificar la fecha, hora y duración de una comunicación; iv) identificar el tipo de comunicación; v) identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; vi) identificar la localización del equipo de comunicación móvil"* (Directiva 2006/24/CE, 2006, L 105/57). En un primer momento, en el articulado de la propuesta se hacía una referencia más genérica a los datos a conservar y se detallaba en un anexo, con la prevención de que podría modificarse por el procedimiento de comitología[156]. No obstante, ante la oposición tanto del GT29, como del resto de instituciones y organismos que opinaron sobre las propuestas (Comité Económico y Social, Supervisor Europeo de Protección de Datos y Parlamento Europeo) finalmente se mantuvo la redacción que indicamos al comienzo del párrafo (en el artículo 5).

- Otra cuestión destacable es la relativa a las medidas para garantizar una correcta conservación de los datos desde el punto de vista de su seguridad. En este punto, nos referiremos únicamente a la prevención que Vilasau (2006; 9)[157] menciona con acierto, y con la que estamos de acuerdo, al analizar el contenido del artículo 8 de la Directiva [que establece los datos deben estar almacenados de tal forma que puedan ser enviados sin demora a las autoridades solicitantes]:

[156] Comitología es un término usado en el ámbito de las instituciones europeas que se refiere a los procedimientos a través de los cuales la Comisión Europea ejerce las competencias que le confiere los Tratados para la ejecución de los actos legislativos en el ámbito de la Unión Europea.

[157] VILASAU, M., *"La Directiva 2006/24/CE sobre conservación de …"*, op. cit. p. 9

"resulta preocupante que el principal objetivo de la conservación adecuada fuera facilitar el acceso a los datos a las autoridades y no el de garantizar los derechos de los afectados. Si bien este aspecto se ha corregido un poco en el texto definitivo, es revelador de la filosofía que late bajo la Directiva[158]*"*.

- Otra cuestión de gran relevancia y que tuvo consecuencias claras en las sentencias del Tribunal europeo, es la relativa al procedimiento de acceso a los datos por las autoridades nacionales competentes. La Directiva, en su artículo 4.2 deja a criterio de los Estados miembros, en las correspondientes normativas de transposición, el establecimiento del procedimiento concreto y las condiciones precisas para tener acceso a los datos. Aunque cita de forma expresa que se deberán cumplir con los requisitos de necesidad y proporcionalidad, de acuerdo con el derecho de la Unión y, en particular, el Convenio Europeo de los Derechos Humanos y de los Tribunales correspondientes, los órganos consultivos que opinaron al respecto exigían que el acceso y tratamiento se produjera solo en casos específicos y con control de una autoridad judicial (sin perjuicio de los países en los que se prevea también que ese control sea ejercido por una autoridad independiente); además, deberían quedar registros claros de los accesos producidos. No obstante, estas *sugerencias* no fueron tenidas en cuenta.

- Una discusión clásica en el ámbito de las negociaciones de expedientes legislativos en la Unión Europea es el de los períodos de conservación de los datos; en este caso, se cumplió el mismo patrón. Las autoridades policiales tradicionalmente abogan por periodos de conservación que sean lo más largos posibles y alguna institución concreta -como es el Parlamento Europeo- defiende la necesidad de plazos más acotados. Muchas veces, según la experiencia de quien redacta este documento, se tiende a encontrar

[158] El SEPD, en el punto 62, junto a otras consideraciones relativas a la transmisión de los datos (no revelar otros datos distintos de los datos necesarios a efectos de solicitud), afirmaba que "*los proveedores deben instalar el entramado técnico necesario, incluidos motores de búsqueda, para facilitar el acceso directo a los datos específicos"*. ¿Realmente esta última media supone una tutela de los ciudadanos?

el acuerdo en el punto medio. En este caso, aunque el papel del Parlamento Europeo no era el mismo que a partir de la entrada en vigor del Tratado de Lisboa [abundaremos en esta cuestión más adelante], se cumplió el mismo patrón. En concreto, se estableció un margen temporal entre seis meses y dos años, sin especificar distinción en función del tipo de dato de que se trate. Se dejó en manos de los Estados miembros, a través de sus normas de transposición, la posibilidad de modular los plazos en función del tipo de dato u otras circunstancias.

- Respecto del borrado de los datos al finalizar el plazo de conservación -según lo recogido en las respectivas normas nacionales, de acuerdo con lo expuesto en el párrafo precedente- la Directiva no habla del procedimiento para hacerlo ni de posibles sanciones en el caso de no llevar a cabo estas acciones; solo pide que se destruyan cuando finalice el plazo.

- Por último, una de las cuestiones que producían rechazo en el sector profesional afectado, como lo es siempre que se negocia un instrumento legislativo en el ámbito de la Unión Europea, es el de los costes que se generan por la adopción de las nuevas medidas. En este caso, el sector de las telecomunicaciones debía asumir costes derivados de la obligación de conservar los datos requeridos, de establecer mecanismos para su transferencia a las autoridades nacionales competentes y por las medidas de seguridad que debían establecer sobre los datos conservados. La Directiva, aunque en la propuesta de la Comisión se incluía un apartado concreto al respecto, finalmente no lo incorporó al texto definitivo y lo dejó en manos de cada Estado miembro. El efecto inmediato fue no cumplir con la armonización pretendida, al menos en este aspecto que consideramos relevante, especialmente en la seguridad de los datos conservados y el mal uso que se podría hacer de ellos si llegaban a manos de quienes no estaban autorizados ni habilitados para ello. En este sentido, Rodotà (2006; 58) pone de manifiesto también el peligro que corremos cada uno de los titulares de

los datos ante el hecho de que éstos puedan ir a parar a manos de alguien que los obtenga ilegalmente[159].

El mismo autor (Rodotà, 2006; 56)[160] resume las cuestiones anteriores en *"tres tendencias convergentes y todas ellas restrictivas de la intensidad de la protección de los datos: tendencias hacia la totalidad [conservación de todos los datos], la permanencia [de seis meses a dos años, ampliable] y la disponibilidad de las informaciones recogidas [referencia genérica a delitos graves y a autoridades nacionales competentes]"*.

A pesar de todo lo anterior, el mismo año de su aprobación, cuando aún estaba comenzando el periodo previsto para la transposición a las normativas nacionales, Irlanda interpuso en julio de 2006 recurso contra la Directiva, argumentando que una medida destinada a la lucha contra la criminalidad y el terrorismo[161] no podía basarse en el Tratado de la Comunidad Europea.

En 2014, el Tribunal de Justicia de la Unión Europea dictó sentencia, en los *asuntos acumulados C-293/12 y C-594/12*, conocida de forma breve como *Caso Digital Rights Ireland Ltd.*, declarando inválida la Directiva 2006/24/CE, por considerar que constituía una injerencia de gran magnitud y especial gravedad en los derechos fundamentales relativos a la privacidad y a la protección de datos. En definitiva, fue invalidada porque infringía el principio de proporcionalidad recogido en el artículo 52.1 de la Carta de los Derechos Fundamentales de la Unión Europea. Argumenta Ballaschk (2015; 21), siguiendo el criterio de Hert y Papakonstantinou, que *"esta sentencia ilustró la fragilidad e inestabilidad de las medidas que chocaban con el derecho de la protección de datos y la necesidad de cerrar la brecha entre la UE y sus ciudadanos*

[159] RODOTÀ, S.,*" La conservación de los datos de tráfico en las comunicaciones…"*, op. cit., p. 58. Pone como ejemplo el robo en 2005 de los datos de 52 millones de clientes de Mastercard en EE. UU., que llevó al Senado de ese país a aprobar una ley que obligaba a los gestores de los bancos de datos a informar a sus clientes de los peligros de los *"robos de identidad"*.

[160] *Ibíd.*, p. 56.

[161] Como hemos indicado ya anteriormente, son materias del Tercer Pilar.

pudiendo superar de esta forma el déficit de confianza en este ámbito"[162]. Más adelante nos detendremos de forma pormenorizada en esta importante cuestión y *desmenuzaremos* esa sentencia y las que la siguieron. Desde luego, podemos adelantar que se ha producido un cambio de paradigma que aún no ha encontrado solución satisfactoria para los Estados miembros ni, de forma particular, para sus servicios policiales y otras agencias encargadas de la aplicación de la ley.

3.2.2 El *"paquete de protección de datos de 2016"* en la Unión Europea

La producción normativa más reciente de la Unión Europea en materia de protección de datos lo constituye lo que se ha llamado *"el paquete de protección de datos"*, compuesto por un reglamento general y una directiva específica a la que se ha denominado informalmente *"la Directiva Policía"*.

El Reglamento (UE) 2016/679[163] del Parlamento Europeo y del Consejo, de 27 de abril de 2016 es el resultado de un proceso que comenzó en 2009, empujado por el rápido avance de las tecnologías y la necesidad de aportar uniformidad al régimen de protección de los datos personales; no obstante, la propuesta de la Comisión se retrasó hasta 2012 y las discusiones se alargaron en el tiempo, por la dificultad de alcanzar consenso en el seno de las instituciones europeas. Se publicó en el año 2016 y entró en vigor en mayo de 2018. Al mismo tiempo, se presentó también una propuesta de directiva, la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016[164] que sustituía a la Decisión Marco 2008/977/JAI del Consejo. El objetivo era (obviamente) adaptarse a los desafíos actuales relativos a la protección de los datos personales, fortaleciendo la privacidad y, aunque es un objetivo más reciente, impulsar también la economía digital de la Unión Europea.

A las actividades de las fuerzas y cuerpos de seguridad y a las autoridades judiciales, en su labor de persecución y enjuiciamiento del delito, les afecta

[162] BALLASCHK, J., *"In the unseen realm: transnational intelligence sharing in the European Union- Challenges to fundamental rights and democratic legitimacy"*, Standford Journal of International Law, 51, 2015, pp. 19-51.

[163] Conocido como Reglamento General de Protección de Datos.

[164] Conocida como Directiva Policía.

principalmente la Directiva 2016/680, aunque aquellas otras actividades que queden fuera de ese ámbito concreto estarán sujetas al reglamento y no a la Directiva. A diferencia del reglamento, la Directiva no se aplica directamente, sino que debe transponerse a la legislación nacional y, para ello, otorgaba un plazo de 24 meses, que finalizó el 6 de mayo de 2018. No todo tratamiento de datos personales con fines policiales y de seguridad pública es acorde en estos momentos con la Directiva 2016/680, puesto que contiene disposiciones que permiten la adaptación en el futuro: entre otros, los actos jurídicos correspondientes a los sistemas especiales de tratamiento automatizado de datos de los Estados miembros en el ámbito del derecho penal y la seguridad pública (Korff y Georges, 2018; 69)[165]. El artículo 63, apartado 1 posibilita que un Estado miembro podrá prever, excepcionalmente, cuando ello suponga un esfuerzo desproporcionado, que los sistemas de tratamiento automatizado creados antes del 6 de mayo de 2016 se ajusten a lo dispuesto en el artículo 25, apartado 1, a más tardar el 6 de mayo de 2023; o incluso demoras mayores, en determinadas circunstancias especiales, en un plazo que no podrá ser posterior al 6 de mayo de 2026 (Directiva 2016/680, 2016, L119/131).

De la misma manera, en virtud de la Directiva 2016/680 (contrariamente a lo que ocurría con la Decisión Marco del Consejo, de 2008) el cumplimiento de las normas y acciones de la Unión y de los Estados miembros en materia penal y de seguridad pública necesita ahora estar justificado. Esto quiere decir que se realizarán controles para comprobar que se cumplen con los criterios establecidos, incluido el que se cumplan las salvaguardas correctas de protección de datos, así como que la transferencia de datos, en base a un interés público, no exceda la protección de los derechos y libertades fundamentales de las personas propietarias de los datos personales afectados.

Por consiguiente, en Europa, tanto la Unión Europea como el Consejo de Europa han revisado o actualizado recientemente[166] sus principales normas en la materia.

[165] KORFF, D., y GEORGES, M., *"Guía para delegados de Protección de Datos…", op. cit.*, 69.

[166] Entre los años 2016 y 2018.

Estamos de acuerdo con Rebollo Delgado (2008; 14)[167] en que *"no puede negarse que la regulación en Europa, tanto de la vida privada, como del derecho a la protección de datos personales, tiene el nivel más alto de reconocimiento y garantía"*. Las últimas normas adoptadas, a las que nos hemos referido, le dan (nos dan) la razón hoy en mayor medida. En el ámbito jurisdiccional, tanto el Tribunal Europeo de Derechos Humanos (TEDH) como del Tribunal de Justicia de la Unión Europea[168] también han ampliado su doctrina en este ámbito. Estas mejoras legislativas han requerido de consensos no siempre fáciles de alcanzar y con redacciones complejas, pero han producido efectos positivos en la vida de los ciudadanos europeos y en la actividad de las personas jurídicas. Como contrapartida, han tenido también una incidencia notable -muchas veces de forma negativa- en el trabajo de las autoridades policiales y judiciales en su labor de lucha contra el terrorismo y la delincuencia grave.

[167] REBOLLO DELGADO, L., *Vida privada y protección de datos…,* op. cit. 14.

[168] Hasta diciembre de 2009, se llamaba *"Tribunal de Justicia de las Comunidades Europeas - TJCE"*.

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

Hasta ahora, hemos estudiado el derecho a la protección de los datos personales, pero aún no hemos definido qué entendemos por datos personales y cómo los trata la normativa europea. Consideramos que, una vez establecidas las bases de la protección del derecho, podemos dar un paso más y adentrarnos en el objeto de la protección y sus diferentes variantes.

Como dijimos al analizar la regulación jurídica europea sobre la protección de los datos personales, el Convenio nº. 108 del Consejo de Europa estableció que por datos de carácter personal había de entenderse *"cualquier información relativa a una persona física identificada e identificable"*, que llamó *"persona concernida"*[169]. Este convenio, actualizado en 2018, varía solo ligeramente la definición, pero sí cambia la denominación de la persona concernida, que ahora llama *"titular de datos o interesado"*. Por su parte, la Directiva 95/46/CE recogió que por *"datos personales"* se entendía *"toda información sobre una persona física identificada o identificable"*, que en su caso denomina de forma diferente al convenio, como *"interesado"*. La más reciente norma de la Unión Europea en la materia, el Reglamento General de Protección de Datos, se refiere al titular de los datos como *"el interesado"*.

Como acertadamente identifica Polo Roca (2021; 216) [170], tenemos dos tipos de datos personales, los correspondientes a una persona identificada y los que pueden llevar a identificar a una persona -persona identificable. El Reglamento General de Protección de Datos recoge en su artículo 4 que:

> *"se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de*

[169] Art. 2 del Convenio nº. 108 del Consejo de Europa.

[170] POLO ROCA, A., *"Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos"*, en Estudios de Derecho, ISSN 0423-4847, ISSN 2386-9062, Vol. 69/1, enero-junio 2021, pp. 211-240, en http://www.revista-estudios.deusto.es

localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (Reglamento 2016/679, 2016; L 119/33).

Por consiguiente, siguiendo la argumentación de Polo Roca, cuando nos referimos a una persona identificable, nos referimos a un dato que no indica de forma directa la identidad de esa persona, pero con la utilización de determinados medios, procedimientos y quizás tecnología, podemos llegar a conocer su identidad. En cambio, una persona identificada lo es porque el dato nos permite de forma directa conocer su identidad sin necesidad de otros medios adicionales o complementarios. El Grupo del Artículo 29 aporta otra definición que resume lo expuesto respecto de una persona identificable: *"aquella persona física que, aunque no se le haya identificado todavía, sea posible hacerlo"*. La identificación, por tanto, puede ser directa -persona identificada- o indirecta -persona identificable[171]. En la identificación también influye el contexto, como así ha reconocido el GT29, que en su Dictamen 4/2007 sobre el concepto de datos personales, dice que las circunstancias concretas del caso influyen en que se identifique o no una persona concreta[172].

El Tribunal de Justicia europeo también se ha pronunciado sobre el concepto de dato personal, reconociendo que es muy amplio. Considera el alto Tribunal, en su Sentencia en los Asuntos C-434/16 y C-582/14[173], que no es necesario que la información que permite la identificación de una persona esté en poder de un único individuo, ya que los medios que lo permiten pueden estar al alcance de muchas personas. El TEDH también lo ha tratado en diferentes momentos, definiendo lo que

[171] Una persona puede ser identificada directamente por su nombre y apellidos e indirectamente por un número de teléfono, el número de la SS, el DNI, etcétera, o por una combinación de determinados criterios: empleo, domicilio, lugar de nacimiento, edad, etcétera.

[172] Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 20 de junio, p. 14.

[173] Sentencia del TJUE, de 20 de diciembre de 2017, asunto C-434/16, Peter Nowak y Data Protection Commissioner, ap. 31 y Sentencia TJUE, de 19 de octubre de 2016, asunto C-582/14, Patrick Breyer y Bundesrepublik Deutschland, ap. 43. A modo de ejemplo, para el TJUE, constituyen datos personales tanto el nombre de una persona, como su número de teléfono y cualquier otra información relativa a sus condiciones de trabajo o a sus aficiones; así como datos de movimientos bancarios, los que obran en poder del municipio, los perfiles creados en una red social, o los que figuran en el registro del lugar de trabajo, o la imagen grabada por una cámara, etcétera. Como no, también la dirección de correo electrónico, si contiene datos que identifican el nombre de la persona, o los datos que permiten la localización del terminal telefónico. También la dirección IP de un ordenador.

considera que son datos relativos a la vida privada y familiar, ya que en el Convenio Europeo de Derechos Humanos no existe el reconocimiento al derecho de protección de datos de forma autónoma, sino ligado a la vulneración del derecho a la vida privada y familiar, según se recoge en el artículo 8 del Convenio.

La pregunta que nos haríamos a continuación, que se hizo Polo Roca (2021; 221)[174] de forma muy pertinente es acerca del *"dato no personal"* -por contraposición al personal- y su protección. Su *"impersonalidad"* no excluye su protección, si bien no será bajo el ámbito de la normativa de protección de datos que hemos venido analizando, sino quizás en el ámbito de protección del derecho al respeto a la vida privada y familiar que recoge el artículo 8 del CEDH.

Los datos de tráfico y de localización que rodean a las comunicaciones electrónicas no son *inofensivos*; todo lo contrario, aportan una información que puede generar peligros evidentes a la hora de recopilarlos, almacenarlos, tratarlos y transmitirlos, provocando consecuencias sobre determinados derechos de sus titulares, que ya hemos analizado. Pueden aportar información sobre quiénes han estado en contacto de diferentes maneras -mensajes, correos electrónicos, llamadas, etcétera-, en qué momento y de qué forma, lo que, adecuadamente tratado, puede revelar hábitos y comportamientos precisos de la vida cotidiana de las personas, incluso de aquellos que puedan ser especialmente sensibles. Pueden también establecer la red de relaciones de una persona y conocer su forma de pensar, su forma de expresarse o participar en un determinado grupo o colectivo. Como revela Fernández Rodríguez (2016; 96)[175], puede incluso incidir en la libertad de expresión de las personas, en la medida en que "*un individuo que sabe que se recaban esos datos puede autocensurarse a la hora de efectuar una comunicación o de establecer ciertas iniciativas públicas.* González de la Garza (2004; 277)[176] sostiene el mismo argumento: *"resulta difícilmente discutible el efecto disuasorio que representa para cualquier ciudadano manifestar sus expresiones*

[174] POLO ROCA, A., *"Datos, datos, datos: el dato personal, el dato no personal…"*, op., cit., 221

[175] FERNÁNDEZ RODRÍGUEZ, J.J., *"Los datos de tráfico de comunicaciones electrónicas: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente"*, Revista Española de Derecho Constitucional, Centro de Estudios Políticos y Constitucionales, 2016, pp. 93-122, p. 96.

[176] GONZÁLEZ DE LA GARZA, L.M., *Comunicación Pública en…op. cit*., p. 277.

libremente cuando sus datos de tráfico están siendo almacenados sistemáticamente y sin excepción". También puede afectar a sus movimientos, pues otro de los datos que se generan es producido gracias a los sistemas de localización que ofrece el GPS que la inmensa mayoría de los dispositivos actuales tienen instalado por defecto.

La Directiva 2002/58/CE sobre privacidad electrónica sigue en vigor[177]. Como ya adelantábamos, establece normas estrictas para garantizar un alto nivel de protección de los datos de las comunicaciones electrónicas, pero permite a los Estados miembros fijar restricciones y limitaciones y adoptar medidas que prevean la conservación de datos por un determinado tiempo. Eso sí, todas las medidas mencionadas *deberán ser conformes con los principios generales del Derecho de la UE*.

Dentro de esas posibilidades es donde se enmarca la aprobación de la Directiva 2006/24/CE de conservación de datos, que establecía normas específicas para armonizar las medidas en la materia en toda la Unión. Sin embargo, fue invalidada por el Tribunal en 2014, en una sentencia que será la base principal de los siguientes capítulos. La declaración de nulidad fue *"ex tunc"*, es decir, se retrotrae hasta la fecha en que esta entró en vigor: 2006.

Una vez que la Directiva quedó anulada, se presentó otro caso ante el Tribunal de Luxemburgo para evaluar la conformidad con la Carta de la legislación nacional [en este caso la sueca] adoptada sobre la base del artículo 15, apartado 1 de la Directiva sobre privacidad electrónica y, en su sentencia de 21 de diciembre de 2016, dictaminó que el artículo 15, apartado 1 *"leído a la luz de la Carta, debe interpretarse en el sentido de que se opone a una legislación nacional que, con el fin de luchar contra la delincuencia, prevé la conservación general e indiscriminada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados a todos los medios de comunicación electrónica"*[178].

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

[178] Vid. Nota del Servicio Jurídico del Consejo al COREPER (doc.5884/17).

Esta doctrina tuvo y tiene actualmente implicaciones directas para las capacidades operativas de las autoridades policiales y judiciales competentes en lo que respecta a garantizar la disponibilidad y el posterior uso de los datos conservados con fines de prevención, investigación, persecución y enjuiciamiento de los delitos, especialmente respecto de los delitos graves. El TJUE también planteó la necesidad de abordar el panorama disperso de las normas de conservación de datos en aquel momento [y actualmente] aprobadas en toda la Unión.

Por otro lado, y estrechamente relacionado, en 2017 la Comisión Europea presentó una propuesta de reglamento sobre la privacidad y las comunicaciones electrónicas[179], cuyo objetivo y características fueron expuestos por esta institución al Consejo de la Unión Europea en julio de ese año. Los Estados miembros participantes en el grupo de trabajo correspondiente[180] acordaron que, además de una legislación específica sobre la retención de datos [si así era decidido por la Comisión] podría considerarse también un enfoque complementario con el objetivo de garantizar la disponibilidad de los datos de tráfico y de localización de las comunicaciones que los operadores recogen y tratan con fines comerciales, evitando de esa forma imponer al sector afectado una obligación como tal de almacenamiento con fines de prevención y persecución del delito en el proyecto de reglamento[181].

A pesar de las reticencias y diferencias de parecer habituales entre los diferentes actores en torno a las discusiones tras la presentación de cualquier borrador de reglamento [o directiva], [el borrador de reglamento de privacidad electrónica] sí mantiene que los Estados miembros pueden limitar por ley determinadas obligaciones y derechos, *"siempre que tal limitación constituya una medida necesaria y proporcionada para proteger determinados intereses públicos como la seguridad*

[179] "Comisión Europea (2017), Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)", COM (2017) 10 final, Bruselas, 10 de enero de 2017.

[180] Grupo de Trabajo de Telecomunicaciones (WP TELE, por sus siglas en inglés), en el ámbito del Consejo de la UE.

[181] Esta idea se desarrollará con profundidad en los capítulos siguientes.

nacional, la defensa, la seguridad pública y la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la sanción de infracciones penales"[182] (Propuesta de reglamento privacidad comunicaciones electrónicas, 2017; 27). De ese modo, *"los Estados miembros podrían mantener o crear marcos nacionales de conservación de datos que previeran medidas de conservación específicas, siempre que dichos marcos fueran conformes al Derecho de la Unión, habida cuenta de la jurisprudencia del TJUE sobre la interpretación de la Directiva sobre privacidad y las comunicaciones electrónicas y de la Carta de los Derecho Fundamentales"*[183] (Propuesta reglamento privacidad comunicaciones electrónicas, 2017; 3).

1. La conservación de los metadatos en las comunicaciones electrónicas

Aunque ya nos hemos referido a este término en diferentes ocasiones, es en este momento cuando nos proponemos profundizar en el concepto de *"metadatos"*. El Diccionario de la Real Academia Española no recoge una definición de metadato. En cambio, el Diccionario panhispánico del español jurídico sí la contempla[184]:

> *"descripción estandarizada de las características de un conjunto de datos. En el contexto del documento electrónico, cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento".*

Esta definición no es del todo válida a los efectos de la materia que estamos tratando, por lo que creemos más aconsejable recurrir al concepto en inglés; así, según el diccionario de Oxford: *"a set of data that describes and gives information about other data".* Se trata de una agregación de información, de la información alrededor de

[182] En el Considerando 26.

[183] Ver la exposición de motivos de la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, COM (2017) 10 final, punto 1.3.

[184] Recogida del Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso.

una determinada actividad y que, según el Consejo de Derechos Humanos de las Naciones Unidas[185], puede arrojar información sobre comportamientos, relaciones o preferencias de una persona, incluso de forma más precisa que con el contenido de una comunicación privada [recordemos que la Directiva 2006/54/CE no afecta al contenido de las comunicaciones electrónicas]. Los metadatos afectan a muchas y muy importantes *actividades* de la vida cotidiana de los ciudadanos; sin embargo, nos interesan especialmente los que proceden o se producen por las comunicaciones electrónicas entre individuos.

El tratamiento de los metadatos y su agregación pueden permitir establecer perfiles de personas; no solo identificarla, sino conocer detalles de su intimidad y su vida privada. Cita Polo Roca (2021; 226)[186] el estudio que llevaron a cabo Jonathan Mayer, Patrick Mutchler y John C. Mitchell, que demostró que solo con los metadatos se pudo saber, además de la identidad de una persona, alguna de sus enfermedades, que tenía armas de fuego, e incluso que había abortado (Mayer, Mutchler y Mitchell, 2016; 113)[187].

Según la diferenciación que hemos establecido entre *datos personales* y *datos no personales*, los metadatos serían considerados dentro de la segunda categoría y, en consecuencia, no estarían bajo el amparo de la normativa de protección de datos. Sin embargo, en la doctrina creada por el Tribunal de Justicia de la Unión Europea a través de la declaración de nulidad de la Directiva 2006/24/CE, se concede a éstos la misma protección puesto que, considerados en su conjunto, constituyen datos personales, que permiten conocer muchos detalles de la vida privada.

[185] Ver el informe de la Oficina del Alto Comisionado para los Derechos Humanos del Consejo de Derechos Humanos (CDH) de las Naciones Unidas, sobre el derecho a la privacidad en la era digital, de 30 de junio de 2014, A/HRC/27/37, nº. 19

[186] POLO ROCA, A., *"Datos, datos, datos: el dato personal, el dato no personal…"*, op., cit., 226.

[187] Para ampliar datos del estudio, vid. *"Evaluating the privacy properties of telephone metadata"*, de Mayer, Jonathan, Mutchler, Patrick y Mitchell, John C., 2016, en Proceedings of the National Academy of Sciences of the United States of America (PNAS), 113, nº 20, en https://doi.org/10.1073/pnas.1508081113

Otra cuestión relevante que requiere de análisis es la que, de forma muy pertinente, plantea Fernández Rodríguez (2016; 102)[188], acerca de si deberíamos partir de analizar si es necesario o no conservar [estamos usando de forma indistinta también el término retener; por la traducción del inglés *"retention"*] *"los datos de tráfico [y de localización] por razones de seguridad"*.

Para responder a esta cuestión, recordemos lo expresado ya acerca de que los ciudadanos realizan cada vez más actividades y transacciones cotidianas utilizando redes y servicios de comunicaciones electrónicas, y todos y cada uno de los movimientos a través de estas redes generan una serie de datos que permiten a los proveedores de servicios de comunicaciones electrónicas cumplir con una serie de funciones administrativas y comerciales[189]; datos entre los que se incluyen detalles sobre la hora, el lugar y los números utilizados para los servicios de voz fijos y móviles, correos electrónicos, mensajes de texto y otros cada vez más extendidos usos de internet. Por su parte, los datos de los abonados y, en ocasiones, de los usuarios, como el nombre y la dirección, también son tratados por los proveedores a efectos de gestión de las suscripciones. En definitiva, por motivos técnicos y mercantiles, los proveedores de servicios deben conservar durante un determinado espacio temporal algunos de esos datos; en resumen, una ingente cantidad de información. Para tal fin, se entiende y no se cuestiona que las empresas del sector de las telecomunicaciones necesitan esos datos para poder prestar el servicio, cobrarlo y reaccionar ante errores, quejas o sugerencias. Por poner como ejemplo a España [ya indicamos que en algunos momentos sería necesario, para ilustrar mejor nuestra argumentación], la Ley 9/2004, de Telecomunicaciones, permite el tratamiento de los datos de tráfico *"a efectos de la*

[188] FERNÁNDEZ RODRÍGUEZ, J.J., *"Los datos de tráfico de comunicaciones electrónicas…"*, op., cit., p. 102

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

- *Los datos que constituyen el contenido de los mensajes enviados durante la comunicación y que son estrictamente confidenciales;*
- *Los datos necesarios para establecer y mantener la comunicación -los llamados metadatos, que en la Directiva reciben el nombre de "datos de tráfico"-, como la información relativa a las partes de la comunicación, la hora y la duración de la comunicación;*

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

transmisión de la comunicación" y los necesarios *"a efectos de la facturación de los abonados y los pagos de las interconexiones"* hasta que *"expire el plazo para la impugnación de la factura del servicio, para la devolución del cargo efectuado por el operador, para el pago de la factura o para que el operador pueda exigir su pago"*.

Para proteger determinados derechos y libertades fundamentales de los ciudadanos, la legislación comunitaria prevé [y también la española] la supresión de esos datos *(o su "enmascaramiento"*[190]*)* una vez que ya no son necesarios para la transmisión de la comunicación.

Más allá de los fines comerciales, también pueden invocarse objetivos de *"seguridad u orden público*[191]*"* para justificar el tratamiento ulterior. No cabe duda de que la disponibilidad de estos datos puede ser importante para determinados fines policiales y judiciales: como la investigación, persecución y enjuiciamiento de conductas delictivas graves. Por ello, las autoridades de los Estados miembros podían (en principio, si era necesario) de acuerdo con la legislación aplicable a nivel nacional, solicitar el acceso a los datos de localización y tráfico (metadatos) almacenados por los operadores para sus fines empresariales. Las solicitudes de retención de datos específicos también estaban permitidas cuando eran necesarias para esos mismos fines específicos, garantizándose así el almacenamiento posterior de datos de usuarios concretos a partir de la fecha de solicitud.

Sin embargo, con los cambios en los modelos de negocio y las ofertas de nuevos servicios, como tarifas planas, servicios de prepago o incluso gratuitos, los operadores dejaron de guardar determinados datos de tráfico que ya no eran necesarios para su labor de gestión interna y cuyo almacenamiento suponía costes adicionales. Esta

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

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

tendencia se vio reforzada notablemente tras la aparición de la voz sobre IP y los servicios de tarifa plana. Parece obvio que, si los datos no se almacenan, no estarán disponibles para las autoridades cuando haya un caso legítimo para acceder a ellos. En otras palabras, estos avances dificultaban mucho el cumplimiento de las funciones que corresponden a las policías y autoridades judiciales en materia de prevención y lucha contra la delincuencia grave y el terrorismo y, al mismo tiempo, facilitaban a los delincuentes la comunicación sin temor a que los datos de sus comunicaciones pudieran ser utilizados para frustrar sus acciones, investigarlas y enjuiciarlas.

Para responder a esta preocupación, varios Estados miembros aprobaron medidas generales de conservación de datos a nivel nacional, lo que llevó a la Unión Europea a plantear una solución legislativa europea, apoyada en la declaración del Consejo Europeo de 2004, que reconoció explícitamente la importancia de las medidas legislativas sobre la retención de datos de tráfico e instó al Consejo de la Unión Europea a examinar opciones y plantear propuestas. De hecho, también constataron los jefes de estado y de gobierno de los Estados miembros de la Unión que era un asunto urgente e incluso fijaban un plazo máximo para la adopción del nuevo instrumento legislativo (para antes de junio de 2005). La prioridad concedida a la adopción de un instrumento jurídico adecuado fue confirmada posteriormente por las conclusiones del Consejo Europeo de 16 y 17 de junio de ese mismo año, así como en la reunión especial del Consejo JAI[192] de 13 de julio de 2005, tras los atentados terroristas en Londres.

Es un criterio compartido tanto por los representantes políticos como diplomáticos, y también entre los expertos, que en la lucha contra el terrorismo no puede actuarse de forma individual, y en esto no hay fisura alguna en las discusiones en el seno del Consejo de la Unión Europea. Por lo tanto, a nivel político se convierte en un objetivo de interés general y así ha sido reconocido también por el propio Tribunal

[192] Consejo de ministros de Justicia e Interior de la Unión Europea. Reúne de forma periódica, en sesiones formales, informales y extraordinarias a los ministros de justicia y de interior de los Estados miembros y, para determinados asuntos concretos, también a los de los Estados asociados a Schengen, con el objetivo de elaborar políticas de cooperación y comunes sobre diferentes cuestiones transfronterizas, con la finalidad de crear un espacio de libertad, seguridad y justicia en toda la Unión Europea.

de Justicia de Luxemburgo[193]. No analizaremos aquí el contenido de ninguna sentencia sobre esta consideración [apoyo] del Tribunal, porque no es un criterio que haya sido cuestionado por este en la sentencia de 2014 por la que invalidó la Directiva 2006/24/CE, ni las subsiguientes que confirman su doctrina.

En la lucha contra la delincuencia grave y organizada se pueden usar los mismos argumentos que justifican la necesidad de garantizar el derecho a la seguridad de los ciudadanos en una sociedad democrática y de libre convivencia, según recoge el artículo 6 de la Carta de Derechos Fundamentales de la Unión Europea. De ahí que exista un interés general que justifica la injerencia que la conservación de datos provoca en otros derechos y, por otro lado, se asume que esos datos (metadatos) son útiles para contribuir a garantizar el derecho a la seguridad, mediante la investigación de los delitos graves, la averiguación de sus autores, etcétera, que lleven a su enjuiciamiento y a la aplicación de sanciones penales.

Al mismo tiempo, el Tribunal europeo también ha dictaminado que la conservación constituye una injerencia en los derechos fundamentales [que ya hemos mencionado en reiteradas ocasiones] tanto si estos son sensibles como si no lo son[194]. De ahí que surja *tensión* entre ambos derechos que lleva a la búsqueda de un adecuado equilibrio entre los intereses en juego. Como indica Fernández Rodríguez (2016; 104)[195], citando al filósofo Zygmunt Bauman: *"nadie ha encontrado todavía en la historia y en el planeta la fórmula de oro para la mezcla perfecta de seguridad y libertad"*[196]. Seríamos muy pretenciosos si pensáramos que vamos a encontrar esa fórmula a través de esta tesis, siquiera para el caso concreto que nos hemos propuesto

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

[194] TJUE, Caso Rechnungsfof contra Österreichischer Rundfunk y otros, y Christa Neukomm y Jospeh Lauermann vs. Österreichischeer Rundfunk, en Sentencia de 20 de mayo de 2003, apartado 75).

[195] FERNÁNDEZ RODRÍGUEZ, J.J., *"Los datos de tráfico de comunicaciones electrónicas…"*, op., cit., p. 104.

[196] Vid. diálogo entre Fernando Schüler y Mario Mazzilli, en https://www.youtube.com/watch?v=in4u3zWwxOM.

estudiar; empero, no renunciamos a aportar algunos elementos que puedan mejorar el proceso de búsqueda de la deseada y esquiva fórmula.

2. Los metadatos y su contribución a la labor de investigación penal

Para comprender por qué el Consejo Europeo y un número significativo de Estados miembros pidieron medidas de conservación de datos, es necesario conocer la importancia de estos para las investigaciones penales. En este contexto, durante el proceso de consulta previo a la presentación por la Comisión de una propuesta de directiva, las autoridades policiales pusieron ejemplos concretos de la contribución que el acceso y tratamiento de esos datos supuso para el buen fin de las investigaciones y enjuiciamiento de los responsables.

La facultad de Derecho de la *Universidad Erasmus de Rotterdam* presentó el 20 de junio de 2005 un estudio público[197] sobre la necesidad de que las fuerzas de seguridad tuvieran acceso a los datos. El estudio se centró en 65 casos diferentes en los que los datos de tráfico de las telecomunicaciones habían desempeñado un papel relevante y confirmó su importancia para todo tipo de investigaciones, incluidos delitos tan graves como los de terrorismo, o asesinatos y secuestros. Especialmente en los casos de secuestro, los datos sobre la ubicación de un dispositivo móvil desempeñan a menudo un papel crucial. También confirmó que cuanto más importante es el caso, más larga es la investigación y, por tanto, más antiguos son los datos que se solicitan. De hecho, sugiere que, especialmente las investigaciones sobre delincuencia organizada grave -como fraudes de gran envergadura- o los casos que implican solicitudes de asistencia jurídica mutua, o los llamados *casos sin resolver* y el terrorismo son los que más se benefician de un periodo de conservación más largo.

En el estudio también se proporcionan ejemplos en los que los datos ya se habían borrado cuando la solicitud llegó al proveedor de servicios, como en un caso de asesinato en Francia. Las autoridades policiales de otro Estado miembro indicaron que,

[197] *"Wie wat bewaart die heft wat"*; traducido con DeepL.com y consultada el 11.07.21 en http://www.europapoort.nl/9345000/1/j9vvgy6i0ydh7th/vgbwr4k8ocw2/f=/vh1iiavsmqwi.pdf.

de las solicitudes de datos relacionados con Internet, entre el 30 y el 40% quedaban sin respuesta porque los datos ya se habían borrado.

La ciberdelincuencia[198] sigue siendo una amenaza creciente, que socaba la confianza en el desarrollo del comercio electrónico y contribuye a perjudicar los intereses de los ciudadanos y de las empresas mediante ataques a los sistemas de información, fraudes y robos de identidad o la distribución en línea de pornografía infantil, por poner solo algunos ejemplos.

Algunos expertos policiales han comparado los metadatos con las huellas dactilares: *"mientras que en el mundo físico se pueden recoger huellas físicas, en el mundo digital los datos de tráfico y de localización son el equivalente digital a las huellas digitales"*[199].

Aparte de los importantes daños monetarios causados por la ciberdelincuencia, internet también ha creado amplias oportunidades para la distribución y venta de pornografía infantil. En un caso concreto, las autoridades policiales de un Estado miembro encontraron direcciones IP de personas que descargaban pornografía infantil de internet; posteriormente se realizaron detenciones en 12 Estados miembros, basadas en esas direcciones IP. Sin embargo, en otros 5 Estados miembros, esas direcciones IP ya no pudieron vincularse a usuarios individuales, puesto que los datos correspondientes ya habían sido borrados por los proveedores de servicios de internet.

Por otro lado, las investigaciones sobre delitos graves -como la delincuencia organizada o el terrorismo- son casi automáticamente investigaciones internacionales, dada la naturaleza de las organizaciones implicadas. Esto significa a menudo que hay

[198] Entendida en este estudio como los actos delictivos que se cometen usando las tecnologías de la información y la comunicación para atacar redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito.

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

que recurrir a los mecanismos de la cooperación internacional, ya sea utilizando los métodos tradicionales de asistencia jurídica mutua, o mediante el uso de las posibilidades que ofrecen agencias como Europol o Eurojust. Zapater Duque (2014; 101)[200] refiere que precisamente la globalización de la criminalidad ha favorecido también la centralización de instituciones, en aras a prevenir y combatir de forma más eficaz determinados delitos y, en ese contexto es en el que también Europol ha incrementado sus relaciones con terceros Estados y, de esa forma, ha contribuido al desarrollo de la dimensión exterior del ELSJ. No obstante, incluso con la mayor rapidez que proporcionan estas instituciones para solicitar e intercambiar la información pertinente, es evidente que estos procedimientos llevan tiempo. Si los datos no se conservan durante un período de tiempo razonable, las solicitudes de acceso no serán operativas: para cuando la solicitud llegue al operador a través de la correspondiente autoridad, es muy posible que los datos se hayan borrado[201].

Mientras que la declaración sobre la lucha contra el terrorismo y la declaración del Consejo sobre la respuesta de la UE a los atentados de Londres demuestran claramente el compromiso político de adoptar medidas legislativas adecuadas en la Unión sobre la retención de datos, el dilema de cómo alcanzar el equilibrio adecuado entre los derechos fundamentales a la protección de la vida privada y de los datos personales, y las necesidades del Estado de disponer de instrumentos adecuados para salvaguardar la vida, la libertad y la propiedad de sus ciudadanos ya se refleja en el marco jurídico actual, y en particular en la Directiva 2002/58/CE. Sin embargo, la Directiva de 2002 no prevé una armonización de las condiciones en las que las medidas legislativas nacionales pueden prever la conservación de datos con fines de investigación y persecución del delito. Si bien esta circunstancia deja cierta discrecionalidad a los Estados miembros sobre el nivel exacto de protección que pretenden garantizar en su territorio utilizando la excepción que prevé el artículo 15,

[200] PI LLORENS, M. y ZAPATER DUQUE, E., *La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia*, Marcial Pons, Madrid, 2014, p. 101.

[201] Un ejemplo de caso internacional, facilitado a la Comisión durante las consultas, se refiere a un ataque contra un sitio web del Gobierno de los Estados Unidos, que dio lugar a una solicitud de asistencia jurídica mutua, a través de la cual se pidió la identificación de los usuarios de cuatro direcciones IP. Aunque en este caso el período de tiempo transcurrido entre la recepción de la solicitud y la actuación fue de poco más de un mes, la identificación de los usuarios de las cuatro direcciones IP no fue posible porque los datos correspondientes ya habían sido borrados por los proveedores de servicios de internet afectados.

apartado 1 de la Directiva de 2002, no exime a las posibles medidas nacionales de la verificación de su respeto a las obligaciones que les incumben en virtud de esa directiva y del derecho comunitario en general, incluida la obligación de respetar los derechos fundamentales y los principios generales del derecho de la UE sobre los que ya nos hemos pronunciado (consagrados en la Carta y en el Convenio Europeo de Derechos Humanos).

Sin embargo, en aquel momento existía toda una variedad de obligaciones nacionales de conservación de datos en los Estados miembros, que pueden resumirse como sigue:

- La mayoría de los Estados miembros no tenían obligaciones de conservación de datos;
- En aproximadamente la mitad de los Estados miembros con leyes obligatorias de conservación de datos, s no eran operativas, ya que no contaban con medidas de aplicación;
- En los Estados miembros que tenían obligaciones de conservación de datos, el período y el alcance variaban sustancialmente, por ejemplo: sólo los móviles de prepago, no para internet, para todos los servicios, etcétera.

En resumen, el problema que pretendía abordar la Directiva sobre conservación de datos era que las autoridades policiales estaban perdiendo de *forma lenta, pero segura*, uno de sus instrumentos más importantes para prevenir y combatir la delincuencia grave y el terrorismo. La situación era, por tanto, insatisfactoria en cuanto a la respuesta a las graves preocupaciones expresadas por el Consejo Europeo y, en cuanto a las consecuencias de las medidas divergentes adoptadas por los Estados miembros, para la eficacia de la cooperación internacional en materia de aplicación de la ley; pero también para los proveedores, especialmente los que prestan servicio en diferentes Estados miembros de la Unión.

Al margen del devenir posterior, la UE adoptó la Directiva y consideró que se cumplía con los criterios de necesidad y proporcionalidad; circunstancia que después

fue cuestionada por el TJUE. Ya en 2004, en el análisis del proceso de aprobación del proyecto de Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI)[202], González de la Garza (2004; 339 y ss.)[203] estudió el devenir que este texto tuvo en la Comisión encargada de su redacción y concluyó lo siguiente -que se asemeja en gran medida a lo que más tarde puso en cuestión el TJUE respecto de la Directiva 2006/24/CE:

"Esta norma, en efecto, tiene un carácter fiscalizador extremo de la libertad de expresión e información…. Constituye una medida desproporcionada en un Estado democrático y consideramos que responde…, a un efecto patológico adverso de los atentados terroristas del 11 de septiembre del año 2001 en los Estados Unidos. La lucha en los Estados democráticos para salvaguardar los derechos fundamentales y las libertades públicas de la injerencia irrazonable de los poderes públicos en la vida privada e intimidad de las personas experimenta, con normas como la recientemente aprobada LSSI en nuestro país, retrocesos injustificables, basados en riesgos genéricos y difusos que precisan siempre y en todo caso la demostración de que las medidas a adoptar restrictivas de derechos fundamentales o limitativas de los mismos han de ser justificadas y meridianamente claras, sometidas a su vez a plazos temporales breves, que en ningún caso se perpetúen temporalmente más allá de lo inmediata y estrictamente necesario".

En abril de 2011, la Comisión presentó un informe de evaluación sobre la Directiva de conservación de datos[204] y en sus conclusiones señalaba:

> *"La mayoría de los Estados miembros consideran que las normas de la UE sobre conservación de datos siguen siendo necesarias como herramienta para la aplicación de la ley, la protección de las víctimas y los sistemas de justicia penal. Las pruebas facilitadas por los Estados miembros en forma de estadísticas y ejemplos son limitadas en algunos aspectos, pero no obstante son muestra del importante papel que desempeñan los datos conservados en la investigación penal. Estos datos proporcionan valiosas pistas y pruebas en la*

[202] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Para profundizar, vid. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

[203] GONZÁLEZ DE LA GARZA, L.M., *Comunicación Pública en*…, op. cit. pp. 339-340.

[204] Vid. COM (2011) 225 final.

prevención y enjuiciamiento de delitos y para garantizar la justicia penal. Su utilización ha dado lugar a condenas por delitos que, sin la conservación de datos, nunca podrían haberse resuelto. También ha dado lugar a sentencias absolutorias de personas inocentes" (Informe de evaluación de la Comisión, 2011; 38).

En definitiva, en un entorno político y geoestratégico como el actual, con múltiples amenazas y riesgos, clásicos y emergentes, la lucha contra el terrorismo y la delincuencia grave y organizada se han convertido en una prioridad de primer orden para las agendas políticas de los Estados miembros de la Unión Europea de forma individual, y para la propia Unión Europea en general. Empero, [aunque no debería ser necesario ponerlo de manifiesto] esa *lucha* debe ser necesariamente respetuosa con el ejercicio y disfrute de los derechos fundamentales y las libertades y, para ello, habrá que determinar los límites precisos sobre unos y otros, basándose en el establecimiento de medidas necesarias, apropiadas y proporcionadas, según reza el artículo 15, apartado 1 de la Directiva 2002/58/CE[205]. Este artículo indica que las medidas que se adopten serán *"conformes con los principios generales del derecho comunitario"*, citando los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea; y ese artículo remite a la Carta de Derechos Fundamentales de la Unión Europea y al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que ya hemos citado en pinas anteriores.

Esta habilitación jurídica dio lugar a la Directiva 2006/24/CE, cuya tramitación y aprobación fue muy controvertida, como hemos ya señalado. Considera Fernández

[205] Artículo 15.1 de la Directiva 2002/58/CE del Parlamento y del Consejo, de 12 de julio de 2002: *"Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea"*.

Rodríguez (2016;108)[206], como otros muchos autores, que quizás el legislador no estuvo acertado al optar por una directiva y basarse en un desarrollo de la libertad de circulación de servicios en vez de acudir al Espacio de Libertad, Seguridad y Justicia, que podría haber prestado más atención a las garantías sobre los derechos afectados. La propia Comisión Europea, en el informe de evaluación de la aplicación de la Directiva de 2011 que hemos citado, ponía de manifiesto que la conservación de datos había demostrado ser útil a los efectos de investigación y persecución de delitos graves, pero reconocía también críticas respecto del respeto a la intimidad[207]. En ese momento, la Comisión anunciaba la intención de modificar la legislación para reforzar el sistema de conservación de datos, su acceso y tratamiento. Los acontecimientos posteriores y el pronunciamiento reiterado del Tribunal de Justicia de la Unión Europea cambiaron el panorama notablemente y generaron una nueva situación que se extiende hasta nuestros días.

[206] FERNÁNDEZ RODRÍGUEZ, J.J., *"Los datos de tráfico de comunicaciones electrónicas…"*, op., cit., p. 108.

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

CAPÍTULO IV. EL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA COMO GARANTE DE LOS DERECHOS DE LOS EUROPEOS

A modo de introducción, antes de abordar la materia que da título al presente capítulo, esbozaremos las características principales que interesan a los efectos de nuestra tesis sobre las tres instituciones europeas fundamentales. Ya hemos citado a la Comisión Europea, al Parlamento Europeo y al Consejo de la Unión Europea en repetidas ocasiones antes de llegar hasta aquí, pues son instituciones de las que se habla cotidianamente y cualquier lector puede identificarlas perfectamente, al menos en cuanto a sus generalidades. Ahora, pretendemos explicar con algo más de detalle lo que representan y a quiénes sirven, además de su participación en la adopción de políticas europeas y en el procedimiento de producción normativa, y lo haremos especialmente para resaltar algunas características concretas que nos permitan entender la interrelación entre ellas, de cara a vislumbrar qué *falló* a la hora de aprobar la Directiva 2006/24/CE y qué podemos aprender de ese *error* que tuvo que enmendar el Tribunal de Luxemburgo. De la participación de estas tres instituciones nace la normativa que conforma el derecho de la Unión Europea, bajo el papel de intérprete de que ejerce el Alto Tribunal de Luxemburgo.

La *Comisión* se puede considerar como el gobierno de la Unión Europea, puesto que representa los intereses de con absoluta independencia respecto de los Estados miembros y del resto de las instituciones europeas. Esta característica le permite ser la fuente de producción normativa en cuanto a que tiene la capacidad de elevar propuestas sobre las materias que le otorgan los Tratados y, de esa forma, ofrecer una visión completa y de conjunto sobre políticas concretas. Para materias sobre las que no tiene competencia exclusiva, puede proponer medidas de armonización de las legislaciones nacionales, a través de determinados instrumentos normativos que veremos en su momento. Aunque, como decíamos, es independiente de los Estados miembros, el hecho de que, en la configuración actual, haya un comisario por cada uno de los países miembros, pretende lograr un equilibrio adecuado en la representación de éstos en su órgano de dirección (el colegio de Comisarios), en la idea de que así, en cierta medida, sus políticas se alineen con la voluntad de los estados. Esto no siempre ha sido de esta forma y tampoco era necesario, si consideramos que los comisarios, independientemente de su país de origen, debían gozar de plena libertad e

independencia para desarrollar su labor en favor de los intereses de la Unión Europea[208]. Sin embargo, los recelos propios de una organización política como es la Unión Europea, que todavía no ha llegado a su grado de madurez óptima, hacía pensar lo contrario a los Estados miembros y mostraban recelos ante la elección incluso de varios comisarios de un mismo país; por tanto, la forma más europea de solucionar esas desavenencias fue la paridad y, por tanto, la elección de un comisario por Estado miembro. A medida que se han ido adoptando nuevos tratados, se ha variado la dinámica sobre qué número de comisarios debe ser el adecuado y si se deben establecer rotaciones entre países para no aumentar en exceso la cifra, pero todavía hoy están representados cada uno de los Estados miembros[209]. La relevancia de esta particularidad está en el hecho de que es una muestra clara del déficit de confianza de los gobiernos de los Estados miembros hacia las instituciones comunitarias, puesto que no solo está el hecho de querer contar con un representante en el órgano directivo de la Comisión, sino que también se pretende acceder [controlar] las carteras más relevantes, en términos de visibilidad y, sobre todo, de manejo de una mayor porción del presupuesto comunitario, quizás en la idea de que eso repercutirá en mayor medida en políticas de interés del país de procedencia del comisario concreto[210].

Como poder ejecutivo, la Comisión se encarga también del cumplimiento por los Estados miembros del derecho comunitario, mediante el seguimiento de la aplicación correcta de la normativa europea y, en el caso de las directivas, con la observancia del deber de transposición en tiempo y forma a las legislaciones nacionales. Para ello, cuenta con un instrumento de corrección que permite la imposición de sanciones económicas y administrativas a aquellos países *incumplidores*, tras la sustanciación del correspondiente procedimiento sancionador. Desde la adopción del Tratado de Lisboa, la Comisión tiene también la facultad de presentar recursos contra los Estados

[208] El artículo 213.2 del Tratado de las Comunidades Europeas exigía que estos no recibieran instrucciones de ningún gobierno ni lo solicitaran.

[209] La última modificación que se ha hecho, con la salida del Reino Unido de la UE, ha sido la de reducir el Colegio de Comisarios en un miembro y que sus competencias sean asumidas por otro comisario.

[210] Hemos asistido en España de forma recurrente a este debate, considerando que no hemos contado con un comisario que ocupe una cartera relevante o que gestione gran parte del presupuesto. Actualmente, el representante español en el Colegio de Comisarios es el Sr. Josep Borrell, que si bien se creyó en el momento de su nombramiento que tendría mucha visibilidad, pero no dirigiría una cartera con manejo de presupuesto, ahora, por la invasión de Ucrania, se ha convertido en una cartera relevante y no solo decorativa.

miembros ante el Tribunal de Luxemburgo[211]. No solo efectúa propuestas normativas, también emite otro tipo de decisiones no legislativas, en forma de recomendaciones y dictámenes.

El *Consejo*, en cambio, representa los intereses de los Estados miembros, que no siempre coinciden con los de la Unión Europea en su conjunto, como organización política. De hecho, esta función tiene que ver con el equilibrio entre la representación de los intereses nacionales y los comunitarios (que defiende la Comisión). La representación de cada país se ostenta, dependiendo del nivel de la reunión de que se trate, por un miembro del gobierno nacional con rango de ministro (para configuraciones sectoriales) o el propio presidente del gobierno o jefe de estado (según el país de que se trate). Por lo que se refiere a la presidencia del Consejo, se asume de forma rotatoria, con periodicidad de seis meses y siguiendo un turno previamente establecido y, salvo cambios extraordinarios, se repite con la misma cadencia [esto hace que se pueda saber a largo plazo cuándo corresponde la presidencia a cada país, salvo en el caso de nuevas incorporaciones de países a la UE, que alteraría el orden; o, aunque menos frecuente, pero también se ha producido, porque algún país la abandone, como ha ocurrido con el Reino Unido[212]]. Plantea Fernández Ogallar (2014; 93)[213] que se ha cuestionado la falta de legitimidad de los representantes de los Estados miembros en el Consejo por no haber sido elegidos directamente por los ciudadanos, pero determinados autores encuentran esa legitimidad en el hecho de que los representantes son miembros de los gobiernos que han sido elegidos democráticamente en elecciones nacionales, y asemeja esta situación a las segundas cámaras de los estados federales, donde se da una legitimidad indirecta de carácter territorial. Quienes se oponen a este argumento, observan que esa legitimidad lo es solo ante un estado y no frente al resto de los que conforman la Unión Europea. Igual que la Comisión, también ha sufrido variaciones, en este caso no solo en el número de miembros [a medida que se han ido incorporando nuevos socios], sino también en la ponderación de los votos necesarios para alcanzar las mayorías y las materias para las que se requiere mayoría simple o cualificada, que

[211] Artículo 265 del TFUE.

[212] En el momento de la salida del Reino Unido de la Unión Europea, estaba próxima la presidencia británica y se otorgó su puesto a Croacia.

[213] FERNÁNDEZ OGALLAR, N., *El derecho penal armonizado en la Unión Europea*, Madrid, Dykinson, 2014, p.93

actualmente están otorgados en función del tamaño, población y poder político y económico de cada miembro.

El *Parlamento* representa de forma directa los intereses de los ciudadanos europeos, pues son ellos quienes eligen a sus representantes en un proceso electoral que se celebra cada cinco años. Los europarlamentarios se agrupan en la cámara por ideologías y no por nacionalidades[214] y votan de forma personal e individual, sin *sometimiento* a disciplina de partido. Su principal función es la legislativa, aunque no de forma autónoma, sino compartida con el Consejo y ante propuestas de la Comisión Europea.

La competencia principal del Parlamento que nos interesa a los efectos de este estudio es el de constituirse en elemento clave en la aprobación de las normas europeas, especialmente en las que actúa como colegislador con el Consejo, aunque no es un poder exento de límites, debido a la función también relevante del otro colegislador y a que no tiene autonomía para proponer propuestas, sino que necesita que estas nazcan de la Comisión. En definitiva, no tiene capacidad para aprobar propuestas propias, sino que tiene que instar a la Comisión (como también lo hace el Consejo) a presentar una propuesta sobre alguna materia concreta de competencia exclusiva de la Unión o compartida con los Estados miembros. Como en el caso de las otras dos instituciones, el número de parlamentarios ha ido variando con el tiempo y la adopción de los sucesivos tratados, buscando un sistema que recoja la proporcionalidad del reparto de escaños en relación con la población del Estado miembro. Parece obvio, sin miedo a equivocarnos, que no es fácil olvidarse del país de procedencia y del partido político nacional de pertenencia y, en consecuencia, la representación en el Parlamento Europeo tiene efectos claros a la hora de ejercer la función legislativa que le corresponde según los tratados comunitarios.

La función principal a los efectos que nos interesan es la de ejercer el poder legislativo como órgano codecisor junto con el Consejo, ante el ejercicio de la iniciativa

[214] Para evitar interferencias de sus países de origen.

normativa que corresponde a la Comisión. Lo relevante es que, el Tratado de Lisboa ha reforzado esa capacidad del Parlamento y en el actual procedimiento legislativo ordinario, tiene el mismo peso que la otra institución. Esta situación no satisface plenamente a la Cámara, que sigue insistiendo en reforzar su posición frente al resto de las instituciones europeas, como representante de la voluntad de los ciudadanos.

Al *Tribunal de Justicia* le corresponde la potestad jurisdiccional en la Unión Europea, según recoge el artículo 19.1 del TUE, lo que le confiere legitimidad en la interpretación y aplicación del derecho comunitario y en la armonización de las normas en ámbitos compartidos con los Estados miembros, como son las materias de derecho penal. Está compuesto por un magistrado por cada Estado miembro, buscando legitimidad a través de la igualdad en la representación de cada país, lo que a nuestro juicio indica, una vez más, desconfianza ante *lo europeo* y que es necesario avanzar todavía en gran medida para mejorar el crédito que los ciudadanos conceden a las decisiones que se adoptan en el seno de las instituciones europeas. Consideramos que en una situación de clara consolidación de la Unión Europea [tanto para este caso como para los que hemos visto anteriormente -nombramiento de comisarios o funcionamiento del Consejo de la Unión Europea, o de elección y participación de los europarlamentarios] se deberían seguir otros criterios distintos a los de representación proporcional o igualitaria de los Estados miembros, sin cuestionar que estas adolecerán de falta de imparcialidad o de politización de las decisiones que los representantes de estas instituciones tomen en sus respectivos ámbitos de actuación.

El Tribunal se articula en salas, compuestas por tres o cinco magistrados, entre los que se designa a uno de ellos como presidente. No obstante, también se puede constituir una Gran Sala, según establece el artículo 251 del TFUE, cuando sea solicitado por algún Estado miembro o una institución europea que sean partes en el proceso en el que se suscite su intervención. También puede actuar en pleno, siendo esta una formación de carácter extraordinario reservada para los supuestos en los que intervenga un asunto de gran relevancia y el Tribunal lo haya decidido así, además de otros supuestos particulares que no vienen al caso.

El Tribunal de Luxemburgo es el máximo intérprete del derecho comunitario y de la validez de las normas que integran su acervo, incluyendo tanto las emanadas directamente de las instituciones europeas como las aprobadas por los Estados miembros en cumplimiento o aplicación de las anteriores, tal y como dispone el artículo 35.1 del Tratado de Maastricht y el artículo 19.1 del TUE en su versión consolidada por el Tratado de Lisboa; lo que se traduce en potestades consultivas, pero también en la adopción de resoluciones vinculantes desde el punto de vista jurídico respecto de los litigios que se susciten en el ámbito de la Unión Europea.

En su labor diaria, es fundamental el mecanismo previsto en el artículo 267 del Tratado de Funcionamiento de la UE, que regula la cuestión prejudicial. Esta permite al juez de un Estado miembro someter a criterio del TJUE aquellos casos en los que tenga dudas sobre la interpretación de un derecho comunitario o sobre su validez a los efectos del proceso que está sustanciando. Argumenta Ugartemendia Eceizabarrena (2017; 382)[215] que es el juez nacional el encargado de tutelar los derechos fundamentales, al actuar como juez de aplicación del Derecho de la Unión, que debe ejercer a través de una relación esencial de cooperación con el TJUE, que se articular principalmente a través de la cuestión prejudicial. Sin embargo, no solo puede recurrir a la cuestión prejudicial un juez [aunque es la vía de acceso más frecuente], sino que también están habilitadas las partes implicadas en el proceso, o hacerlo el propio Tribunal europeo de oficio. Existen casos particulares y excepciones a esta regla general, pero en este caso [en el que no cuestionamos la competencia del TJUE para conocer de los casos planteados sobre la validez de la Directiva 2006/24/CE] solo reseñaremos la especificidad de cómo se insta al Tribunal a pronunciarse sobre la una norma europea. En este supuesto, el juez nacional puede iniciar el procedimiento de consulta ante la instancia europea si así lo estima oportuno; pero no pueden exigirlo las partes implicadas en el proceso, sino únicamente solicitarlo. Cuestión distinta es, como indica Klip (2021; 504)[216], que lo que se suscite ante el juez nacional sea la validez de una norma europea, en cuyo caso este deberá presentar necesariamente la cuestión

[215] UGARTEMENDIA ECEZABARRENA, J. I., UGARTEMENDIA ECEIZABARRENA, J.I., *"La eficacia entre particulares de la Carta de Derechos Fundamentales de la Unión Europea a la luz de la jurisprudencia del Tribunal de Justicia"*, Teoría y Realidad Constitucional, núm. 39, UNED, 2017, pp. 361-386, p. 382.

[216] KLIP, A., *"European Criminal Law, An Integrative Approach"*, 4th Edition, Intersentia, 2021, pp. 121-130.

prejudicial, por cuanto solo el TJUE tiene competencia para juzgar la validez o falta de validez de estas normas.

Respecto de los requisitos para presentar la cuestión prejudicial, no se establece un momento concreto del proceso para hacerlo, ni formalidad alguna respecto de la solicitud, aunque el propio TJUE ha indicado que debería esperarse a que los hechos estén probados, de forma que sirvan de base al pronunciamiento de este y se determine el derecho interno afectado. No obstante, a nuestro entender lo más destacable es que el proceso principal que ha suscitado la consulta deberá suspenderse hasta el pronunciamiento del Tribunal europeo, así como que la resolución afectará no solo al Estado miembro que se ha dirigido a Luxemburgo sino también al resto de miembros de la Unión Europea en la medida en que conozcan de un supuesto idéntico. Sobre los efectos de las sentencias, en el supuesto de declarar la invalidez de una norma europea [como ocurrió en el caso que ha dado lugar a esta tesis], éstos se extenderán desde el primer momento de aplicación de la norma en cuestión (producirá efectos *ex tunc*), si bien el Tribunal podrá valorar y decidir modular o limitar la aplicación retroactiva, basándose en motivos de seguridad jurídica.

No se fija un plazo concreto para dictar resolución, salvo circunstancias especiales, lo que irremediablemente produce un efecto de retraso en la adopción del pronunciamiento por parte del juez nacional que había instado la actuación del Tribunal europeo; circunstancia que ha de ser valorada por el juez nacional a la hora de tomar la decisión de presentar la cuestión prejudicial (salvo en aquellos casos citados anteriormente en que se vea obligado a recurrir al parecer del Alto Tribunal).

El TJUE es competente también para conocer de las violaciones a los derechos fundamentales amparados por la Carta, a instancia tanto de los Estados miembros como de las instituciones europeas; pero también de los ciudadanos, aunque de forma indirecta, por cuanto tendrán que recurrir a la jurisdicción nacional y serán los jueces y tribunales quienes insten al Tribunal de Justicia a pronunciarse si albergan dudas respecto de la potencial lesión de los derechos de los particulares. Sin embargo,

relacionado con esa vulneración de derechos y teniendo en cuenta que puede venir provocada por un acto normativo de las instituciones europeas, el Alto Tribunal puede conocer también de recursos contra actos con efectos jurídicos que emanen de las instituciones europeas con capacidad legislativa, excluyéndose los trabajos previos o preparatorios necesarios a la aprobación de la norma europea y aquellos otros con efectos meramente internos (Mangas Martín y Liñán Nogueras, 2020; 444)[217].

Respecto de los motivos por los que el TJUE podría anular uno de los actos anteriormente mencionados, pueden ser formales o materiales. Los primeros pueden ser declarados de oficio por este por falta de competencia o de potestad de la institución (u organismo para actos no legislativos) o existencia de vicios importantes (como falta de motivación o insuficiencia de esta) o ausencia de consulta a organismos cuando es preceptiva, etcétera. Los segundos, requieren la solicitud de pronunciamiento por parte del Tribunal.

A medida que la Unión Europea ha ido avanzando en integración, se ha producido también un mayor impacto de la normativa comunitaria en la vida los ciudadanos y, de forma lógica, también sobre el ejercicio de los derechos fundamentales que les asisten. Uno de los ámbitos en los que se ha visto esta influencia [quizás de las más acusadas] es el correspondiente a la investigación, persecución y enjuiciamiento de los delitos [de todo tipo, aunque nos incumben de forma particular los delitos graves y aquellos que se enmarcan en el concepto de terrorismo y delincuencia organizada]. De forma paralela, se han ido ampliando las competencias en cooperación policial y judicial, pero también se han reforzado las materias de las que el Tribunal de Justicia de la Unión Europea conoce y se ha mejorado la forma jurídica de la Carta[218]. En definitiva, se ha reforzado su papel como garante de los derechos. Como indica González Pascual: *"en esta tarea el TJUE precisa del TEDH y de los tribunales nacionales, tanto por la escasez de recursos procesales de protección de los derechos en la UE, como por la necesidad de complementar su jurisprudencia con las*

[217] MANGAS MARTÍN , A. y LIÑAN NOGUERAS, D.J, *Instituciones y Derecho de la UE*, Tecnos, 10ª Edición, 2020, p. 444.
[218] En el Tratado de Lisboa.

aportaciones de otros tribunales europeos" (González Pascual, 2014; 960)[219]. Sin embargo, como indica Fernández Ogallar (2014, 124)[220], los Estados miembros han sido siempre cuidadosos a la hora de decidir qué asuntos someten a consideración del Tribunal y, entre ellos, se encuentran los que afectan a materias de derecho penal, por lo que los avances en este sentido han sido tortuosos y lentos. En el caso de España, identifica Tomás Mallén (2017; 456 y ss.)[221] que los Altos tribunales fueron reacios durante un cierto tiempo a plantear sus dudas ante el TJUE, al contario de los ordinarios, que mostraron más disposición a hacerlo; y lo atribuye a un posible "espíritu autorreferencial". Estas cuestiones afectaban fundamentalmente al Tercer Pilar, pero al eliminar el Tratado de Lisboa esa estructura de tres puntos de apoyo, se propicia la extensión de las competencias del Alto Tribunal al derecho penal (entre otros ámbitos) y, en consecuencia, también a su capacidad de actuación sin la previa aceptación de los Estados miembros. Podemos considerar esta circunstancia como de avance hacia la integración europea, pero siguen quedando fuera determinados ámbitos concretos de enorme relevancia, como los citados anteriormente. Volveremos a ello, más adelante.

En ese sentido, el artículo 276 del Tratado de Funcionamiento excluye del ámbito competencial del Tribunal las disposiciones de los capítulos IV y V del Título V de la tercera parte, relativas al ELSJ, respecto de la validez o proporcionalidad de actuaciones operativas de los servicios policiales u otras agencias encargadas de hacer cumplir la ley ni de las responsabilidades de los Estados miembros en el mantenimiento del orden público y la seguridad interior.

El artículo 19 del Tratado de la Unión Europea y los artículos 251 a 281 del Tratado de Funcionamiento constituyen la base jurídica principal sobre el Tribunal de Justicia, y es, como dijimos, una de las siete instituciones fundamentales. Es competente en la jurisdicción de esta y garantiza *"la correcta interpretación y aplicación del Derecho primario y del Derecho derivado de la Unión en su territorio, controlando la*

[219] GONZÁLEZ PASCUAL, M., *"El TJUE como garante de los derechos en la UE a la luz de la Sentencia Digital Rights Ireland"*, en Revista de Derecho Comunitario Europeo, ISSN 1138-4026, nº. 49, Madrid, septiembre/diciembre 2014, pp. 943-971, p. 960.

[220] FERNÁNDEZ OGALLAR, N., *"El derecho penal armonizado…"*, op. cit. p. 124.

[221] TOMÁS MALLÉN, B., *"La ejecución de sentencias del Tribunal de Justicia como responsabilidad compartida: luces y sombras"*, Teoría y Realidad Constitucional, UNED, 2017, pp. 449-481, p. 456 y ss.

legalidad de los actos de las instituciones de la Unión Europea y determinando si los Estados miembros han cumplido las obligaciones que les incumben en virtud de este Derecho" (Europarl, 2021[222]). Asimismo, *"el Tribunal de Justicia interpreta el Derecho de la Unión a petición de los jueces nacionales"*[223]. Así pues, el Tribunal lleva a cabo una labor de equilibrio en los asuntos que se someten a su consideración respecto de conflictos de interpretación del derecho de la UE, tratando de ponderar adecuadamente las circunstancias de cada caso. Desde que comenzó su actividad, son muchos los casos en los que ha tenido que pronunciarse en relación con la protección de los derechos que incumben a esta investigación, de forma que sus sentencias han permitido delimitar, ampliar y, en definitiva, perfeccionar el ordenamiento jurídico de la Unión Europea, aportando criterios que anteriormente eran imaginables.

La inexistencia de un recurso directo a disposición de los europeos ante el TJUE se palía parcialmente mediante la cuestión prejudicial. Sin embargo, hay reticencias a la hora de utilizar esta herramienta jurídica y esto sustrae a los ciudadanos una vía de reparación efectiva sobre la eventual vulneración de sus derechos[224]. Según Sarmento (2004; 53), la cuestión prejudicial no tiene por objetivo principal la protección de los derechos y no es un mecanismo en sí mismo de garantía de los derechos fundamentales, aunque es *"algo más que un instrumento de cooperación; y desde luego algo más que una vía de interpretación y enjuiciamiento de actos comunitarios"*[225]. Para González Pascual (2014; 961), citando a Torres Pérez[226], la jurisprudencia del Tribunal europeo *"precisa de un proceso de deliberación colectiva con las diversas jurisprudencias tanto para alcanzar la madurez y la legitimidad suficientes como para que el propio tribunal se convierta en garante de los derechos en un espacio supranacional"*. Respecto de la protección de los datos personales, si bien existe jurisprudencia abundante del Tribunal

[222] Ver https://www.europarl.europa.eu/factsheets/es/sheet/26/el-tribunal-de-justicia-de-la-union-europea, consultada el 07.07.21.

[223] A través de la figura jurídica conocida como *"cuestión prejudicial"*.

[224] En la Sentencia de 9 de enero de 2001 (1 BvR 1036/99). EuZW 2001, p. 256 (255), el Tribunal Constitucional alemán reconoce que, si la justicia de un país no tiene facultades para proteger los derechos de los ciudadanos frente a actos provenientes de la Unión y no se habilita al Tribunal europeo para conocer de las vulneraciones de los derechos, el ciudadano está indefenso.

[225] SARMENTO, D., *Poder Judicial e integración europea*. *Thomson*, Madrid, 2004, p. 53.

[226] Para profundizar, vid. TORRES PÉREZ, A. *Conflicts of Rights in the European Union. A Theory of Supranational Adjudication*, Oxford University Press, Oxford, 2009, p. 130.

de Luxemburgo, cita la autora (2014; 961) a Saiz Arnaiz[227], quien argumenta que *"la salvaguarda de estos y de la vida privada en el ámbito penal ha sido desatendida por la UE, pero no por el Consejo de Europa y los sistemas constitucionales"*. En ese sentido, asevera con rotundidad González Pascual (2014; 964)[228], refiriéndose a la Directiva 2006/24/CE que *"la única vía para mantener la integridad del Derecho de la UE y preservar los derechos fundamentales era plantear una cuestión prejudicial"*. Analizaremos con más detalle los argumentos que esgrime el Tribunal, por ser directamente aportados en relación con la Directiva de conservación de datos y, por lo tanto, merecer un capítulo independiente. Por su parte, Rizzo (2019; 288)[229] resalta esta decisión del Tribunal como muy relevante, por ser el primer caso en el que anula un acto de Derecho derivado por ser contario a las disposiciones de la Carta de los Derechos Fundamentales de la Unión Europea y en el que no actúa de oficio, sino de la impugnación de uno de los tribunales nacionales.

Como manifestamos, antes del Tratado de Lisboa, el Tribunal europeo recurría de forma frecuente a las sentencias del TEDH, hasta el punto de que, a criterio de muchos expertos, se convirtió en su principal fuente de *inspiración*. El Tratado de Lisboa llevó a la Unión Europea a adherirse al Convenio Europeo de Derechos Humanos, lo que propició su papel [el del CEDH] como fuente de interpretación reconocido en diferentes normas europeas, como son los artículos 6 del TUE[230] y los artículos 52, 53 y el preámbulo de la Carta, de forma que el Tribunal europeo tiende desde entonces más al uso de un criterio propio y ejerce un mayor control de forma autónoma de la legalidad de cualquier intromisión en los derechos fundamentales y del

[227] SAIZ ARNAIZ, A.: *"El Tribunal de Justicia, los Tribunales Constitucionales y la tutela de los derechos fundamentales en la Unión Europea: entre el conflicto y la armonización. De los principios no escritos al catálogo constitucional, de la autoridad judicial a la normativa"*, Constitución europea y Constituciones nacionales. Valencia, Tirant lo Blanch, 2005, pp. 564 y ss.

[228] *"El TJUE como garante de los derechos…",* op. cit. p. 964.

[229] RIZZO, G., *"Derecho a la privacidad y seguridad en el espacio público europeo…", op. cit.*, p. 288.

[230] Art. 6 del TUE: "*La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000…. 2. La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. …. 3. Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales"*.

cumplimiento de los principios de necesidad, proporcionalidad y legitimidad ya sea por particulares o por actuaciones de gobiernos o parlamentos nacionales o europeos.

De eso modo, de acuerdo con González Pascual (2014; 962)[231], la jurisprudencia del TEDH *"coopera en la concreción de los derechos recogidos en la Carta de los Derechos Fundamentales de la Unión Europea al recoger un conjunto de valores y principios comúnmente aceptados por los Estados y no solo sirve de fuente de inspiración del TJUE, sino de determinación de un estándar mínimo"*; a diferencia de momentos anteriores en que más que cooperar, guiaba de forma predominante. El problema surge cuando, a pesar de tratarse de un conjunto de valores comúnmente aceptados por los Estados, la experiencia y la historia de cada uno de ellos también influye, de la misma forma que también lo hace el diferente nivel de *tolerancia* de los ciudadanos ante determinados supuestos o tradiciones nacionales que afectan a los derechos de los ciudadanos y, unas y otras situaciones producen efectos de respuesta diferentes ante la colisión entre derechos. Lógicamente, se ha de buscar siempre un equilibro entre los intereses enfrentados. Traemos esta consideración a propósito de la influencia de estas situaciones o tradiciones respecto de la diferente definición de los derechos, su alcance e interpretación, que refleja las preferencias de los ciudadanos de cada país, así como su comprensión del reparto del poder entre el legislador y los tribunales[232].

En la *Sentencia Pasquale contra Mariella*, el Tribunal europeo aclara que debe responder a las cuestiones prejudiciales que se le plantean, no pudiendo negarse bajo argumentos de falta de pertinencia u oportunidad respecto del asunto inicial. En cambio, sí puede negarse si el asunto planteado está fuera de su ámbito competencial[233]. Respecto de sus decisiones, en la *Sentencia International Transport Workers' Federation et al. contra Viking Line*, en 2007, arguye que puede pronunciarse únicamente en relación con los elementos que constituyen la petición de decisión

[231] GONZÁLEZ PASCUAL, M., *"El TJUE como garante de los derechos…"*, op. cit. p. 962.

[232] DE WITTE, B., *The past and the future role of the European Court of Justice in the Protection of Human Rights*, ALSTON, P., (Ed) The EU and the Human Rights, OUP, 1999.

[233] TJUE, C-244/80, Pasquale Foglia contra Mariella Novello (nº 2), 16 de diciembre de 1981; TJUE, C-467/04, Procedimiento penal entablado contra Gasparini y otros, 28 de septiembre de 2006.

prejudicial, mientras que los tribunales nacionales mantendrán la competencia sobre el litigio original[234].

Desde 1995 se ha consolidado una importante doctrina en relación con la protección de los datos de carácter personal que consagra el artículo 8 de la Carta. El Reglamento general de protección de datos de la UE de 2016 ha recogido los mismos principios y, en consecuencia, la CDFUE sigue siendo adecuada a los efectos de interpretación de los conceptos fundamentales.

De forma particular, respecto de la protección de la privacidad de los ciudadanos europeos, asevera Rallo Lombarte (2017; 584)[235] que:

> *"puesto que el debate sobre la protección de la vida privada se ha visto superado actualmente, en gran medida, por la emergencia del derecho a la protección de datos, […] la protección de tiene sus principales manifestaciones en la garantía efectiva del derecho a la protección de datos frente al fenómeno tecnológico que mayor impacto tiene en los usos sociales: telefonía móvil, Internet y redes sociales".*

Cree también el mismo autor que este derecho a la protección de los datos tiene una clara huella europea que ha sido seguida por otros países a la hora de establecer sistemas y mecanismos de protección semejantes. Del mismo modo, el Tribunal de Luxemburgo se ha convertido también en el garante de primer nivel de la privacidad y de la protección de los datos personales ante esa evolución tecnológica. En este sentido, el Tribunal trata continuamente de buscar un equilibrio entre esos dos principios difícilmente conciliables: la salvaguarda de lo que pertenece a la esfera privada de los ciudadanos y las exigencias de la seguridad marcadas por el aprovechamiento de delincuentes y terroristas de las oportunidades que ofrecen las nuevas herramientas informáticas y las tecnologías de la comunicación, unido al margen de apreciación que

[234] Cf. TJUE, C-438/05, International Transport Workers' Federation y Finninsh Seamen's Union contra Viking Line ABP y OÜ Viking Line Eesti, 11 de diciembre de 2007, apartado 85.

[235] RALLO LOMBARTE, A., *"El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet"*, UNED, Teoría y Realidad Constitucional, núm. 39, 2017, pp. 583-610

los gobiernos y legisladores nacionales -y europeos- tienen en relación con la finalidad antes expuesta: incidir en determinados derechos fundamentales.

Cuando analizábamos la normativa europea sobre protección de los datos, comenzábamos con la Directiva 95/46/CE, y la tomaremos también ahora como punto de partida para estudiar el papel del TJUE en la defensa y garantía de este no tan antiguo derecho fundamental. Según el mismo autor, la Sentencia del Tribunal europeo en el *Caso Lindqvist* (C-101/01, de 6.11.2003)[236] constituye el *"caso de referencia"* en el que el Tribunal confirmó la vigencia de la aplicación de la Directiva a los servicios prestados en Internet, al considerar como tratamiento total o parcialmente automatizado de datos personales la aportación de datos sobre personas y su identificación, y considerar también como tratamiento no personal ni doméstico la difusión de esos datos por Internet a personas desconocidas que acceden a ellos. En este momento nos interesa más quizás otro de los pronunciamientos del Tribunal, cual es (Rallo Lombarte, 2017; 587): *"los conflictos que susciten la protección de datos con otras libertades y derechos merecen un ponderado juicio por parte de las autoridades nacionales que intente evitar el sacrificio de cualquiera de ellos y, en todo caso, verifique el principio de proporcionalidad atendiendo a todas las circunstancias concurrentes en el caso concreto."*[237]

A la han sucedido otras cuestiones prejudiciales que han ido configurando la jurisprudencia del TJUE que, si bien son igualmente relevantes, no requieren de atención por nuestra parte, por cuanto no cuestionamos la competencia ni la importancia de esta institución como garante del Derecho de la Unión Europea en su conjunto, ni en la defensa de la privacidad y la protección de los datos de los europeos, en particular. Sin embargo, no erraremos al aseverar que el concepto actual de los derechos a la privacidad y a la protección de datos en la Unión se deben en gran medida a cómo los

[236] En este asunto se sustancian varias cuestiones prejudiciales sobre la Directiva 95/46 suscitadas en el marco de un proceso penal seguido contra la Sra. Lindqvist, acusada de haber infringido la normativa sueca relativa a la protección de datos personales al publicar en su sitio de Internet datos personales de varias personas que, como ella, colaboraban voluntariamente con una parroquia en Suecia. Fue condenada a una multa por tratamiento automatizado de datos sin autorización, por no comunicarlo previamente a la Autoridad de Protección de Datos y por transferencia internacional de datos a países terceros sin autorización.

[237] RALLO LOMBARTE, A., *"El Tribunal de Justicia de la Unión Europea como juez garante..."*, op. cit., p. 587.

ha ido moldeando el Alto Tribunal, por lo que, como indican García-Valdecasas y Fernández y Carpi García (2004; 32)[238], el derecho a la protección de datos nació de una forma pretoriana, es decir, a través del *ius praetorium*, antes de ser incorporados al derecho.

Aunque más adelante entraremos en el fondo de la cuestión, sí procede mencionar aquí una vez más, aún de forma general, pero con su nombre completo, la Sentencia de 8 de abril de 2014 (*Caso 293/12 y 594/12 Digital Rights Ireland y Seitlinger y otros vs, Irish Data Protection Comissioner*), que anuló la Directiva 2006/24/CE sobre conservación de datos de tráfico y localización de comunicaciones electrónicas que perseguía garantizar la disponibilidad de esos datos con fines de prevención, investigación, detección y enjuiciamiento de delitos graves y, a tal fin, obligaba a los proveedores de servicios a conservar tales datos, así como aquellos otros necesarios para identificar al abonado o usuario[239].

El TJUE aseveró que esos datos, *"agregados o considerados en su conjunto"*, podían arrojar indicaciones muy precisas sobre la vida, hábitos, costumbres, lugares de desplazamiento o frecuentados, etcétera, de la mayoría de las personas y, en consecuencia, producían una injerencia especialmente grave en los derechos fundamentales al respeto a la privacidad y a la protección de datos de carácter personal y generar sentimiento de vigilancia continua y constante. En cierto modo, consideró también que podía producir un efecto negativo sobre los ciudadanos respecto del uso de las tecnologías de la información y las comunicaciones e incluso afectar a su libertad de expresión, que viene recogido en la Carta como otro derecho fundamental, en este caso el artículo 11. En ese sentido, el apartado 37 de la Sentencia[240] lo expresa con el

[238] GARCÍA-VADECASAS Y FERNÁNDEZ, R. y CARPI BADÍA, J.M., (2004), *"El Tribunal de Justicia de la Unión Europea. Algunas consideraciones respecto a su papel en el marco de la construcción europea"*, en Revista Jurídica de CyL, nº. 3, pp. 13-48, p. 32y ss.

[239] Normalmente, al hablar de las sentencias del TJUE, no se menciona el dictamen previo del Abogado General de la Unión Europea, que suelen indicar el sentido de las sentencias, por cuanto el Tribunal no suele apartarse de este en la mayoría de los casos, como sí lo hizo en . El Abogado General fue el español Pedro Cruz Villalón.

[240] Sentencia del TJUE (Gran Sala), de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland Ltd y Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=ES

siguiente tenor: *"la injerencia resulta de gran magnitud y debe considerarse especialmente grave. Además, la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante"*. También concluyó que la injerencia en los derechos fundamentales estaba basada y justificada en razones de interés general, como la lucha contra la delincuencia grave y la seguridad pública, pero no respetaba el principio de proporcionalidad, al tratarse de una injerencia que no se limitaba a lo estrictamente necesario, sino que, al contrario, era de gran magnitud y especialmente grave[241].

Otra Sentencia del Alto tribunal, de 13 de mayo de 2014 *(C-131/12, Caso Google vs. AEPD)*, también merece ser tenida en cuenta en este caso. admitió el *"derecho al olvido"* frente a los buscadores de Internet, que supuso un cambio significativo por cuanto obligó a los buscadores, redes sociales y otros servicios que se prestan a través de Internet a modificar en cierta medida su modelo de negocio, en aras a una mayor privacidad y protección de los datos personales de los usuarios[242]. La injerencia en esos derechos que observa el Tribunal se multiplica debido al papel de Internet en la vida actual; argumento que podemos asemejar también al usado en la *Sentencia Digital Rights*; como también coincide en que un tratamiento inicialmente lícito de datos puede llegar a ser incompatible con los derechos de los ciudadanos cuando éstos se revelen inadecuados, no pertinentes o excesivos atendiendo a los fines para los que fueron tratados y al tiempo transcurrido.

Considera Rallo Lombarte (2017; 600)[243] que en el Caso Google vs. AEPD, *"el Tribunal de Luxemburgo ha sido, ante todo, un juez garante de derechos que ha confirmado la alta condición jurídica que ya venía atribuyéndose a la protección de datos personales tanto en su jurisprudencia como en el marco legal y 'constitucional'*

[241] Apartado 37 de la Sentencia.

[242] Cualquier internauta que realice una búsqueda a partir del nombre de una persona física puede obtener, a través de la lista de resultados, una visión estructurada de la información relativa a esa persona que circula en Internet. De esa forma, los internautas pueden establecer un perfil más o menos detallado de las personas buscadas.

[243] RALLO LOMBARTE, A., *"El Tribunal de Justicia de la Unión Europea como juez garante…"*, op. cit., p. 600.

europeo. El Abogado General reconoce en sus conclusiones ese alcance constitucional derivado de la consagración en los artículos 7 y 8 de la CDFUE del respeto de la vida privada y el derecho a la protección de los datos personales, y no limita su interpretación a un mero juicio de legalidad comunitaria. En definitiva, en este caso [y no es el único] se establece la necesidad de ponderar los derechos afectados, aun cuando todos ellos sean legítimos. A ese respecto, podemos concluir que el TJUE posiciona en un escalón superior los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta.

Por último, otra Sentencia, de fecha 6 de octubre de 2015 *(Caso 362/14 Maximillian Schrems/Data Protection Commissioner), conocido como Caso Facebook)*[244], anuló la Decisión 2000/520/CE de la Comisión Europea de 26 de julio de 2000 que reconocía un nivel de protección adecuado de los datos personales en EE. UU; conocida como *"régimen de puerto seguro" -Safe Harbour, en inglés-*. Esta sentencia afecta a la transferencia internacional de datos, en función del nivel de protección que el país destinatario ofrece en su legislación interna respecto de la privacidad y la protección de los datos personales. En este caso, el Alto Tribunal reconoce de nuevo que los derechos recogidos en la legislación europea deben ser evaluados e interpretados atendiendo a su reconocimiento jurídico en la Carta y, de ese modo, enjuiciarse a la luz del derecho a la vida privada y a la protección de datos reconocidos en los artículos 7 y 8 de esta.

Otro de los aspectos esenciales en la protección de los datos personales reside en la existencia obligatoria de autoridades independientes de vigilancia, que viene recogido en el artículo 8.3 de la Carta; autoridades que dispongan de amplios poderes, facultades y medios para el cumplimiento de su misión de supervisión en los Estados miembros.

[244] Un ciudadano austriaco, Sr. Schrems, usuario de Facebook desde 2008, presentó una denuncia ante la Autoridad Irlandesa de Protección de Datos tras conocer las revelaciones realizadas en 2013 por Edward Snowden en relación con las actividades de la Agencia de Seguridad Nacional (NSA) de Estados Unidos. Conocedor de que los datos de los usuarios de Facebook residentes en la Unión Europea son transferidos a servidores situados en Estados Unidos, el Sr. Schrems motivó su queja en que Estados Unidos no garantizaba una protección suficiente de los datos transferidos a ese país frente a las actividades de vigilancia de sus autoridades. La Autoridad Irlandesa de Protección de Datos desestimó su denuncia entendiendo que la Decisión de la Comisión Europea había estimado el Safe Harbour como un procedimiento de garantía del nivel adecuado de protección de datos. La High Court irlandesa presentó una cuestión prejudicial para evaluar si la Decisión impedía a la Autoridad Nacional de Protección de Datos investigar dicha denuncia.

En este proceso de emancipación respecto del Tribunal europeo de Derechos Humanos, según algunos autores, el TJUE ha alcanzado el papel de un tribunal constitucional europeo con la Carta de los Derechos Fundamentales de la Unión Europea como punto de referencia (Rizzo, 2019; 286)[245], adquiriendo y aplicando una serie de parámetros propios, aunque en realidad es un tribunal particular que interpreta el derecho en una organización de Estados como es la Unión Europea. En ese proceso, según Martínez (2015) [246], ha pasado de la interpretación del Derecho europeo para que no contraviniese las tradiciones constitucionales de los Estados miembros a situar el Convenio Europeo de Derechos Humanos como referente de interpretación y, actualmente, a declarar inválidos los actos jurídicos de las instituciones europeas cuando considera que contravienen la Carta europea.

Seríamos ingenuos sin pensáramos que el complejo equilibrio entre el Derecho nacional de cada uno de los Estados miembros y el de la Unión Europea no continuará inestable. En la práctica, como indica Díez-Hochleitner (2013; 5) [247], en pocos casos está realmente en peligro la identidad constitucional y a través de los mecanismos de cooperación se conseguirá que los derechos estén protegidos en cada caso por el tribunal más adecuado.

1. Breve referencia a la jurisprudencia del TJUE en la lucha contra el terrorismo internacional y su afectación a los derechos fundamentales

En primer lugar, dedicaremos unos párrafos a tratar una cuestión fundamental sobre la que no hay acuerdo general entre los expertos: el alcance de la competencia de la Unión Europea para legislar en el ámbito penal. Si bien el Tratado de Lisboa aclara en cierto modo esta cuestión con la desaparición de los clásicos pilares, la influencia de la Unión Europea sobre el derecho penal en los Estados miembros no es un asunto

[245] RIZZO, G., *"Derecho a la privacidad y seguridad en el espacio público europeo…"*, op. cit., p. 286.

[246] MARTÍNEZ, R., *"Safe Harbor: retos para el modelo europeo de la privacidad"*, en Lefebvre – El Derecho, 19.10.2015, en http://tecnologia.elderecho.com/tecnologia/privacidad/SafeHorbor-modelo-europeo-privacidad_11_874180003.html

[247] DÍEZ-HOCHLEITNER, J., *"El derecho a la última palabra: ¿Tribunales constitucionales o Tribunal de Justicia de la Unión?"*, Papeles de Derecho Europeo e Integración Regional, nº17, 2013, pp. 1-38, p 5.

pacífico. La primera duda que nos surge es la siguiente: *si las competencias de la Unión son por atribución y las materias del Tercer Pilar quedaban fuera de su ámbito de control, al desaparecer esa estructura, ¿las materias que se asociaban a ese pilar (justicia y asuntos de interior) se atribuyen a la UE o sigue desempeñando un papel de búsqueda de una acción común a través de un método de carácter intergubernamental hacia un nivel elevado de protección en un espacio europeo de libertad, seguridad y justicia?* La doctrina no es contundente al respecto. Una parte argumenta que no existe en los tratados ninguna referencia a la capacidad legislativa de la Unión en materia penal, precisamente porque [como hemos argumentado en otras partes del presente trabajo] supone una cesión de soberanía que difícilmente sería aceptable por los Estados miembros. En cambio, otra parte considera que los tratados recogen una serie de metas a alcanzar a nivel comunitario que justificaría la adopción de medidas que lo hagan viable. Esta última afirmación podría justificar la injerencia de las instituciones europeas, principalmente de la Comisión, en la vida de los ciudadanos en una inmanejable variedad de situaciones. Argumentan también los defensores de la segunda opción, que la delincuencia transfronteriza [o el terrorismo de orden internacional] solo puede ser abordada desde una acción concertada a nivel europeo[248]. Esta es la justificación que ha mantenido vivo el debate sobre la necesidad de establecer un derecho penal europeo y una fiscalía europea[249]. En ese sentido, al tratar la propuesta de Directiva relativa al Exhorto Europeo de Investigación en materia penal, defiende Aguilera Morales (2012; 24)[250] que fomentar el reconocimiento mutuo en el ámbito de la investigación penal transfronteriza simplifica y agiliza la cooperación y permite luchar de forma más eficaz contra la delincuencia; sin embargo, cuestionaba en ese momento que hubiera un tratamiento equivalente en los Estados miembros respecto de la protección de los derechos fundamentales y las garantías procesales.

[248] Este argumento se utiliza de forma habitual por la Comisión Europea en las evaluaciones de impacto que acompañan a las propuestas de reglamento y Directivas dentro de la justificación del principio de subsidiariedad: *"que la medida propuesta de que se trate se puede abordar de una forma más eficaz a nivel europeo, que a nivel nacional o regional"*.

[249] De hecho, en 2020 comenzó su andadura la Fiscalía Europea (EPPO, por sus siglas en inglés) que no se puede asemejar a la idea de un ministerio fiscal europeo, por cuanto la EPPO circunscribe su ámbito competencial a determinados delitos económicos y de corrupción que afectan a los intereses financieros de la UE y porque es un instrumento que, precisamente por no ser una competencia exclusiva de la Unión, no participan en él todos los Estados miembros. En consecuencia, se asocia más bien a una medida de cooperación reforzada.

[250] AGUILERA MORALES, M., *"El exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas"*, Boletín del Ministerio de Justicia, nº. 2145, Año LXVI, 2012, pp. 1-29, p. 22, en https://dialnet.unirioja.es/descarga/articulo/3986762.pdf

Por ello, la actuación de la Unión Europea en este ámbito nace de la solicitud de los Estados miembros, expresada en las reuniones del Consejo, a través de sus jefes de estado o de gobierno [o de los ministros de justicia y asuntos de interior, dependiendo del nivel del foro de que se trate]; o por resoluciones o mociones que se aprueban en el Parlamento europeo, a instancia de algún grupo político o eurodiputado; o porque la Comisión observa una necesidad y lo plantea a los Estados miembros y a otros actores interesados, para recoger su parecer. En definitiva, es necesario mostrar a la Comisión alguna *señal* para que esta institución aborde una determina cuestión que pueda culminar en una norma [no siempre tiene por qué hacerse a través de legislación comunitaria] con la idea de armonizar las legislaciones nacionales en la materia y, de esa forma, avanzar hacia la integración europea. Eso sí, una vez que las instituciones han adoptado una norma, respondiendo a la necesidad expresada por los estados, estos tienen que dar cumplimiento a lo acordado y aprobado, puesto que han sido partícipes en el procedimiento, a través de su representación en el Consejo.

Otra cuestión que merece ser destacada es la que determina el margen de maniobra de que disponen los Estados miembros a la hora de cumplir con el mandato otorgado por la Unión a través de la norma europea aprobada, siguiendo la demanda expresada previamente por éstos [seguimos ciñéndonos al ámbito penal]. Para ello, Fernández Ogallar (2014; 174)[251] estudia tres supuestos, dependiendo uno u otro del margen de los Estados miembros para decidir cómo cumplir con la obligación que la norma europea impone:

- Se regula la protección a través del derecho penal de un bien jurídico, especificando el tipo, naturaleza e intensidad de las sanciones a aplicar, lo que no deja margen al legislador nacional, más allá de la trasposición o incorporación al derecho nacional de la legislación europea.
- Se regula la misma protección anterior, pero mencionando que debe realizarse con medidas adecuadas y eficaces. En este caso, se otorga mayor margen a la hora de regular las medidas a nivel nacional.
- Por último, se regula la protección de un bien jurídico con el mismo nivel de protección que el otorgado a nivel nacional. En este supuesto, se confía en la

[251] FERNÁNDEZ OGALLAR, N., *"El derecho penal armonizado…"*, op. cit., p. 174.

legislación nacional y no es necesario aprobar otra específica para adoptar la norma europea[252].

Antes del Tratado de Lisboa [recordemos que se firmó el 13 de diciembre de 2007 y entró en vigor el 1 de diciembre de 2009], con el sistema de pilares, una de las decisiones principales que la Comisión debía tomar era si la propuesta normativa presentada se enmarcaba en el Primer o Tercer pilar, puesto que tenía consecuencias claras e implicaciones directas sobre el tipo de decisión o norma a aprobar y en el papel que desempeñarían las instituciones europeas y las autoridades nacionales. Esta decisión era importante y ayuda ahora a entender una de las cuestiones que más se criticaron de la Directiva de conservación de datos. Puesto que se adoptó en 2006, nació antes del Tratado de Lisboa y, por tanto, es lógico que se suscitara este debate y fuera uno de los puntos criticados por los detractores de la norma. El tiempo les dio la razón. Precisamente, esta norma se basó en el Primer pilar, aunque la mayoría de las cuestiones que regulaba eran del Tercer pilar.

En materias del Primer Pilar se seguía el proceso legislativo de codecisión[253] (ahora llamado procedimiento legislativo ordinario), en el que tanto el Consejo como el Parlamento jugaban un papel paralelo y homogéneo; mientras que en materias de justicia y asuntos de interior el Parlamento ejercía funciones meramente consultivas, como el que se asignaba a otras, como el Comité Económico y Social o el Comité de las Regiones. Por otro lado, si se basaba la medida en el ámbito competencial del Primer Pilar, el expediente se sustanciaba por medio de reglamentos y directivas, mientras que, si se sustentaba en el Tercer pilar, se sustanciará mediante decisiones marco. En esta última circunstancia, además de la participación meramente consultiva del Parlamento, la Comisión tampoco ejercía una labor fiscalizadora similar a la que lleva a cabo con los reglamentos y las directivas actuales. Aun así, volviendo a la materia que da origen a nuestro estudio, antes de la aprobación de la Directiva 2006/24/CE se intentó regular la

[252] Este supuesto se conoce como *"asimilación"*.

[253] En GARZÓN CLARIANA, G., *"El Parlamento Europeo y la evolución del poder legislativo y del sistema normativo de la Unión Europea"*, en Revista de Derecho Comunitario Europeo, nº. 50, enero/abril 2015, pp. 43-83, p. 59, el autor revela que, aunque el Tribunal de Justicia ha acabado por referirse al término "codecisión" en su jurisprudencia, lo cierto es que este término fue evitado en la Conferencia intergubernamental de Maastricht, al objeto de facilitar el acuerdo del Gobierno británico.

conservación de los datos de tráfico y de localización de que disponen los proveedores de servicios de telecomunicaciones, a través de una decisión marco que no prosperó y quizás ese fue el motivo por el que, en un segundo intento, se planteó como una medida de desarrollo del mercado interior, que era un ámbito comunitario enmarcado en el Primer Pilar.

Por último, otra diferencia más entre ambos pilares, importante también a la hora de decidir cómo afrontar la adopción de una medida europea en materia de justicia y asuntos de interior y escapar al *excesivo* control de las instituciones europeas, es que el Tribunal de Justicia europeo gozará de una mayor o menor capacidad de fiscalización (que ya hemos tratado anteriormente).

Sin haber profundizado demasiado en las cuestiones anteriores [consideramos que no es necesario para nuestro trabajo], creemos contar ya con los elementos básicos que nos permitan comprender cómo enfrenta la Unión Europea los asuntos de justicia y de interior y podemos extraer la conclusión de que el control judicial se convierte en la mejor herramienta ante la potencial (o efectiva) extra-limitación de gobiernos o legisladores en la adopción o ejecución de medidas en dos frentes relevantes, íntimamente relacionados pero con características diferentes (quizás los fenómenos más importantes a la hora de aprobar y ejecutar políticas de cooperación en justicia y asuntos de interior): la lucha contra el terrorismo y contra la delincuencia grave. Tanto a nivel de los Estados miembros como en el ámbito de la Unión, los tribunales desarrollan su labor de garantes de la protección de los derechos fundamentales y del ejercicio de las libertades públicas. En la Unión Europea, no es necesario mencionar una vez más quién ejerce esa labor. No obstante, como argumenta Serra Cristóbal (2016; 495)[254], pese a que el TJUE es un *"recién llegado al campo de la lucha contra el terrorismo y otros asuntos de seguridad nacional, si lo comparamos con el TEDH o los tribunales nacionales*, ha tomado ya postura en esta materia. Desde 2014 tiene jurisdicción plena sobre la cooperación policial y judicial en el ámbito penal, aunque esta es limitada sobre

[254] SERRA CRISTÓBAL, R., *"Los derechos fundamentales en la encrucijada…"*, op. cit., p. 495.

la Política Exterior y de Seguridad Común. La *Sentencia Öcalan* [255] recordó que: *"La Comunidad Europea es una comunidad basada en el Estado de Derecho cuyas instituciones están sujetas a revisión judicial de la compatibilidad de su actuación con el Tratado y con los principios generales del Derecho que forman parte de los derechos fundamentales. Por lo tanto, las personas tienen derecho a la tutela judicial efectiva de los derechos que les confiere el ordenamiento jurídico de la Comunidad, y el derecho a esa protección es uno de los principios generales del Derecho que resultan de las tradiciones constitucionales comunes a los Estados miembros […] y en la Convención Europea sobre los Derechos Humanos"* (Caso C-229/05, 2007). El TJUE reconoció que las restricciones nacionales a determinados derechos con la finalidad de luchar contra el terrorismo tienen límites.

Al mismo tiempo, en la defensa de los derechos fundamentales de los europeos debe tener en cuenta también las normas constitucionales de los Estados miembros, la jurisprudencia del CEDH y el resto de los acuerdos internacionales suscritos por la Unión Europea[256]. Diversas sentencias del Tribunal de Luxemburgo han dejado constancia de su pronunciamiento respecto de que las medidas de la Unión Europea en materia de terrorismo deben ser compatibles con los derechos fundamentales; es decir, el Derecho europeo será de aplicación preferente sobre la aplicación de compromisos internacionales. También se ha pronunciado respecto de la obtención de pruebas consideradas secretas en materia de lucha contra el terrorismo y sobre la información que hay que facilitar a un detenido por terrorismo sobre su imputación, aunque las pruebas obtenidas sean consideradas secretas[257].

[255] Sentencia TJUE (Sala Primera), de 18 de enero de 2007, en el asunto C-229/05 P, que tiene por objeto un recurso de casación interpuesto con arreglo al artículo 56 del Estatuto del Tribunal de Justicia, 2l 9 de mayo de 2005.

[256] En el Caso Kadi -Yssin Abdullah Kadi and Al Barakaat International Foundation vs. Council of the European Union and Commission of the European Communities (TJUE. Asuntos acumulados C-402/05 and C-415/05 P, 3 septiembre 2008)- el Tribunal tenía que decidir si una Resolución de la ONU a través de un reglamento europeo constituía una violación clara y evidente de los derechos humanos y que, como éstos deben ser respetados por la UE, no cabía el cumplimiento de aquélla. Kadi fue identificado como un posible defensor de Al-Qaeda por el Consejo de Seguridad de la ONU, se le incluyó en una lista de terroristas y fue sancionado. La Unión Europea transpuso esa sanción de la ONU a través de un reglamento comunitario y fue impugnado por Kadi ante los tribunales europeos, alegando que no había sido informado de los motivos de su inclusión en la lista de personas y entidades sujetas a las sanciones establecidas y, por lo tanto, no había tenido la posibilidad de presentar un recurso judicial contra esos motivos y, en consecuencia, su derecho a ser oído y a una tutela judicial efectiva habían sido vulnerados.

[257] Sentencias en casos C-27/09 P República Francesa vs. OMPI, 2011 y C-300/11 ZZ vs. secretario de Estado del Ministerio del Interior, 2013.

Ha sentado doctrina igualmente en defensa de la intimidad y la privacidad de los europeos en materia de lucha contra el terrorismo [este pronunciamiento nos incumbe de forma directa] en el asunto PNR[258] ante un recurso del Parlamento Europeo sobre el intercambio de información de datos personales de los usuarios de líneas aéreas. El Tribunal anuló la Decisión del Consejo de la Unión Europea que autorizaba la firma de un acuerdo con EE. UU. para que las aerolíneas europeas transfirieran datos personales de sus viajeros; e hizo lo mismo con aquella otra decisión que consideraba que EE. UU. protegía los datos de forma adecuada, al observar en ambos casos que la protección de los datos personales no era adecuada. En definitiva, el Tribunal de Justicia de la Unión Europea no limita su papel de garante de los derechos de sus ciudadanos a las relaciones entre particulares, sino que lo ha ejercido también en la relación entre el Estado y los ciudadanos, en definitiva, entre los poderes públicos y los administrados.

De lo anterior, argumenta Serra Cristóbal (2016; 499-502)[259] que se pueden extraer algunos principios compartidos por los Estados miembros de la Unión en el ámbito de la lucha contra el terrorismo yihadista:

- *"Los derechos y libertades son una prioridad"*. En este momento del trabajo no parece ya necesario aportar justificación para esta aseveración, ni discrepar de ella. La consecuencia directa es la prohibición de su conculcación, salvo que esté justificado de acuerdo con determinados supuestos concretos, pues como indicábamos, ningún derecho es absoluto. Eso sí, la limitación debe ser proporcional (analizaremos a continuación los elementos que forman parte del principio de proporcionalidad).
- *"Incluso en circunstancias excepcionales hay un mínimo de respeto de los derechos fundamentales que debe ser infranqueable".* Los países disponen de recursos que limitan los derechos ante situaciones de emergencia como las que pueden seguir a un atentado terrorista y que conceden amplios poderes a las autoridades. Empero, incluso en estos supuestos se debe ejercer control parlamentario y judicial sobre en qué medida se restringen los derechos.

[258] Sentencia TJUE (Gran Sala) Personal Name Records, asuntos acumulados C-371/04 y C-318/04, de 30 de agosto de 2006.

[259] Analizado con mayor profundidad por la autora.

- *"El respeto por el Estado de Derecho constituye otra lección nuclear extraída del constitucionalismo y compartida por el ordenamiento de la Unión Europea".* Coincidimos con la autora [por otra parte, evidente en el ámbito de la Unión Europea y sus Estados miembros] en que *"cualquier actuación contra el terrorismo que afecte a los derechos humanos tiene que ser adoptada de conformidad con la ley"*.
- *"La eficacia del Estado de Derecho está ligado al principio de rendición de cuentas de las autoridades -tanto judiciales como políticas-".* De esta forma, especialmente referido a las autoridades judiciales, se podrá comprobar la legalidad de las acciones y medidas adoptadas en la lucha contra el terrorismo -y la delincuencia organizada y grave- y el respeto de los derechos y libertades de los ciudadanos.
- *"Los derechos fundamentales imponen obligaciones a los Estados, que son tanto negativas como positivas".* Esta afirmación conecta con el capítulo en el que abordábamos la relación entre libertad y seguridad. Los ciudadanos esperan que los Estados les protejan frente a amenazas graves para la libre convivencia ciudadana, como la que supone el terrorismo y, para ellos, el Estado debe adoptar políticas concretas que no siempre son entendidas o compartidas, pero que siempre deben ser respetuosas de derechos y libertades. Serra Cristóbal (2016; 500)[260] defiende que:

  > *"debemos seguir siendo conscientes del hecho de que la seguridad significa proteger la libertad de las personas, de tal manera que todo el mundo pueda disfrutar de sus derechos sin sentirse amenazado, pero también sin el temor de ser sometido continuamente a limitaciones en sus libertades, especialmente cuando estas limitaciones pueden ser desproporcionadas. Se requiere de un enfoque de la seguridad diferente"*. Esta reflexión es muy interesante y uno de los objetivos que nos hemos planteado, para un caso concreto que afecta a la relación entre la seguridad de los ciudadanos y el libre ejercicio de sus derechos y libertades, mediante la adopción de medidas proporcionadas; sin embargo, no da la autora la clave para conseguirlo, quizás porque, como

[260] SERRA CRISTÓBAL, R., *"Los derechos fundamentales en la encrucijada…"*, op. cit., p. 500.

hemos apuntado en momento anteriores, sea una ecuación sin solución. Intentaremos aportar datos para cada una de las variables con el objetivo de mejorar el equilibrio en el asunto [no menor] al que nos enfrentamos aquí: la conservación de datos metadatos de comunicaciones electrónicas a efectos de aplicación de la ley.

- *"El alcance de los derechos fundamentales ya no es una cuestión reservada a la soberanía nacional".* A esta afirmación de la autora, añadimos que las respuestas en la defensa de esos derechos fundamentales, para el caso del terrorismo yihadista, pero también para múltiples amenazas a la seguridad de los ciudadanos europeos, tampoco puede venir de decisiones o políticas nacionales, quizás tampoco a nivel de la Unión Europea. Respecto del régimen de conservación de datos, fue una decisión europea que se materializó a través de una directiva, posteriormente invalidada por el Tribunal de Justicia de Luxemburgo. Pensamos que la respuesta a la situación generada debe ser también europea [como veremos más adelante], si bien, no podemos afirmar en estos momentos que así vaya a ser, por la evolución de la situación posterior a la sentencia de 2014 y las sucesivas y cómo se ha afrontado el problema por las instituciones europeas encargadas de analizar el contexto actual y las opciones disponibles.

Citamos una vez más una reflexión de la misma autora, que reconoce lo que ya hemos esbozado respecto de la dificultad [casi imposibilidad hasta la fecha] para alcanzar una *"solución de compromiso"* a la tensión entre seguridad y libertad, quedando únicamente margen a algún tipo de equilibrio [inestable]. Estamos de acuerdo con esta afirmación y creemos imprescindible no cejar en el empeño para establecer el ansiado equilibro. Sin embargo, no debemos tampoco olvidar lo referido en momentos anteriores: el punto de equilibrio se detecta y se fija de forma diferente dependiendo de condicionantes previos; es decir, siempre existirá un sesgo, por pequeño que sea, entre quienes priorizan la seguridad por encima de otros derechos igualmente importantes y quienes otorgan a los derechos y libertades civiles un carácter casi ilimitado y absoluto, sin que quede margen alguno para acotar su ejercicio ante supuestos sobre los que también hay que actuar en defensa de otros derechos.

CAPÍTULO V. REQUISITOS PARA UNA INJERENCIA JUSTIFICADA. ESPECIAL REFERENCIA A LOS PRINCIPIOS DE NECESIDAD Y PROPORCIONALIDAD

En el derecho europeo, respecto de la limitación de derechos, es indiscutible (como avala la jurisprudencia del propio Tribunal de Luxemburgo, pero también la del Tribunal Europeo de Derechos Humanos) que deben concurrir razones de necesidad y proporcionalidad, además de preverse ciertas garantías básicas. En el ámbito concreto de la investigación penal y de las actividades enmarcadas en la seguridad pública y nacional hay numerosas sentencias que ilustran estas afirmaciones, anteriores a las que más directamente nos interesan en esta tesis. A modo de ejemplo, como pone de manifiesto Rodríguez García (2013; 235)[261], el *Caso Copland contra UK*, relativo a la interceptación de determinadas comunicaciones electrónicas, llevó al Tribunal Europeo de Derechos Humanos en 2007 a dictar sentencia[262] en el sentido de que la injerencia en el derecho a la intimidad que estas acciones suponían solo se podía considerar necesaria sobre la base de una legislación nacional que lo habilitara. En el *caso S. y Marper contra UK*, sobre la conservación de perfiles de ADN o huellas dactilares de una persona absuelta de un delito o que se haya archivado antes de ser condenado, el mismo Tribunal consideró que la injerencia solo podía aceptarse si la medida respondía a una necesidad social acuciante, que fuera proporcional con el objetivo perseguido y bajo razones pertinentes y suficientes[263]. Indica Tomás Mallén (2014; 232)[264] que *"la jurisprudencia comunitaria se ha basado en la delicada combinación entre el respeto a la privacidad y el déficit de seguridad para decidir la anulación de la legislación europea"*. Un ejemplo de ello, no el único, es el que nos ha llevado a este estudio. En ese sentido, considera la autora que la reciente jurisprudencia del Tribunal confirma la esa doctrina y pone como ejemplo la invalidación de la Directiva de 2006, refiriéndose a la primera de las sentencias (Caso Digital Rights Ireland y otros) por *"excederse [el legislador] en la ponderación de los términos de esta tensión dialéctica"* (2020; 234).

[261] RODRÍGUEZ GARCÍA, L.F., *"La Directiva europea sobre Conservación de Datos de las Comunicaciones Electrónicas y su transposición en el Derecho español"* (2013), Madrid, pp. 235 y ss.
[262] Sentencia TEDH, Copland contra Reino Unido, 3.4.2007, p. 9.
[263] Sentencia TEDH, Marper contra Reino Unido, 4.12.2008, p. 31.
[264] TOMÁS MALLÉN, B., *"Privacidad versus seguridad en el ámbito…",* op. cit. 232.

Roca Trías (2013; 2)[265], refiriéndose a la doctrina española, expone que *"el juicio de proporcionalidad está orientado a resolver conflictos entre derechos, intereses o valores en concurrencia sin necesidad de generar jerarquías en abstracto de los derechos, intereses o valores involucrados y, por tanto, sin necesidad de prejuzgar su mayor o menor legitimidad, ni producir prohibiciones absolutas"*. Figueroa Navarro (1996; 965)[266] también reconoce, al analizar la doctrina y jurisprudencia españolas, que hay acuerdo respecto de que no se puede hablar de jerarquía, sino de equilibrio entre derechos fundamentales y que, en consecuencia, la solución al conflicto entre estos ha de venir por la ponderación, en relación con las circunstancias concretas de cada caso.

Volviendo al Tribunal Europeo de Derechos Humanos[267], aunque los ejemplos citados son solo dos, vemos que muestran los criterios que este Tribunal ha fijado en su doctrina y que señalábamos antes: el requisito previo de una necesidad social acuciante para considerar que la intromisión sea proporcionada con el fin legítimo que se persigue[268]. En su valoración de la necesidad, el Tribunal confronta la medida respecto de la pertinencia e idoneidad con el objetivo perseguido y toma en consideración si esta "*trata de resolver un problema que, de no resolverse, tendría efectos perjudiciales para la sociedad, si existen pruebas de que dicha injerencia podría mitigar dichos efectos perjudiciales y cuáles son los puntos de vista de la sociedad en general sobre el problema"*[269] (Grupo Artículo 29, 2014).

[265] ROCA TRIAS, E., *"Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española"*, XV Conferencia Trilateral, 24-27 de octubre de 2013, Roma, p.2.

[266] FIGUEROA NAVARRO, M.C., *"El conflicto intimidad/información: un análisis jurisprudencial"*, en Anuario de derecho penal y ciencias penales, Tomo 49, Fasc/Mes 3, 1996, pp. 943-978, p. 965.

[267] También conocido como "Tribunal de Estrasburgo" es el Tribunal destinado a enjuiciar, bajo determinadas circunstancias, las posibles violaciones de los derechos reconocidos en el CEDH y en sus Protocolos por parte de los Estados parte de dicho Convenio (ver https://www.echr.coe.int/pages/home) consultada el 01.08.21.

[268] Cf. TEDH, Leander contra Suecia, nº 9248/81, de 26 de marzo de 1987, apartado 58.

[269] Grupo de Trabajo de Protección de Datos del Artículo 29 (Grupo de Trabajo Artículo 29) (2014), Dictamen sobre la aplicación de los conceptos de necesidad y proporcionalidad y protección de datos en el sector de los cuerpos de seguridad, WP 211, Bruselas, 27 de febrero de 2014, pp. 7-8.
Como ejemplo: *"la recopilación y la conservación de datos personales por los servicios de seguridad de determinadas personas que tienen vínculos con movimientos terroristas sería una injerencia en el derecho de las personas al respeto de la vida privada que, no obstante, sirve a una necesidad grave e imperiosa: la seguridad nacional y la lucha contra el terrorismo"*.

La injerencia también tiene que ser *"proporcionada"*. En ese sentido, el TEDH considera la proporcionalidad dentro del concepto de necesidad, que requiere que la injerencia no sobrepase lo necesario para cumplir con el *"fin legítimamente perseguido"*.

La jurisprudencia de este Tribunal fija los siguientes elementos que habrán de ser tenidos en cuenta en el momento de realizar la evaluación del principio de proporcionalidad:

- Alcance de la injerencia y, en particular, en número de personas afectadas;
- Garantías establecidas para limitar su alcance o efectos perjudiciales para los derechos de las personas.

Por su parte, el artículo 52, apartado 1 de la Carta establece que, *"dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando 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"*.

La consecución de un objetivo de interés general puede justificar la adopción de medidas limitativas de los derechos, pero exige, según la jurisprudencia del TJUE, que se produzca una invasión menor que otras a la hora de alcanzar un mismo objetivo; en definitiva, que las limitaciones o excepciones que operen sobre los derechos [al respeto de la vida privada y a la protección de los datos personales] no excedan de lo estrictamente necesario. Indica Troncoso Reigada (2012; 162)[270] que *"el principio de proporcionalidad es clave a la hora de analizar la legitimidad de la publicación de información personal por la Administración, donde es necesario buscar un equilibrio entre el interés público que justifica el acceso a información administrativa y el derecho fundamental a la protección de datos"*. Los inconvenientes y riesgos para el ejercicio de los derechos fundamentales afectados deben estar justificados por unas

[270] TRONCOSO REIGADA, A., TRONCOSO REIGADA, A. *"Hacia un nuevo marco jurídico europeo de la protección de datos personales*". Revista Española de Derecho Europeo, nº 43, julio-septiembre 2012, pp. 25-184, p. 265.

ventajas superiores de las medidas adoptadas, que deben ir acompañadas también de garantías suficientes. Asevera Rizzo (2019; 280)[271], al referirse a la autonomía conceptual del derecho a la protección de los datos personales respecto del respeto a la vida privada, que fue a partir del momento en que el Tribunal de Justicia de la Unión Europea debate sobre las limitaciones a los derechos de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión en relación con el artículo 52, cuando se comenzó a marcar diferencia entre la aplicación del concepto de proporcionalidad y aquel otro relativo a la infracción del contenido esencial de los derechos en litigio.

El Supervisor Europeo de Protección de Datos[272] se pronuncia en términos similares respecto de la necesidad, en sus "*Herramientas para determinar la necesidad* [273]. La Agencia Europea para los Derechos Fundamentales (FRA) considera que la proporcionalidad exige realizar la evaluación teniendo en cuenta todas las circunstancias del caso, la naturaleza, el alcance y la duración de las medidas que determinan la interferencia, especialmente el número de personas afectadas, las razones que subyacen a la autorización, las autoridades competentes y el remedio previsto por la legislación nacional[274]. En definitiva, alcanzar los objetivos con las medidas y medios menos lesivos de los derechos.

El Consejo de Europa también exige evaluar el *criterio de necesidad* ante la injerencia en los derechos fundamentales que puedan verse afectados en aras de garantizar otros derechos y el ejercicio de las libertades de los ciudadanos. Ante un conflicto entre derechos, *"tanto el TEDH como el TJUE han declarado de forma reiterada que es necesario realizar un ejercicio de ponderación con otros derechos en*

[271] RIZZO, G., *"Derecho a la privacidad y seguridad …"*, op. cit., p. 280.

[272] Para ampliar, ver: https://edps.europa.eu/_en?lang=es, consultada el 10.08.21

[273] Supervisor Europeo de Protección de Datos (2017), *"Herramientas para determinar la necesidad",* p.5. (https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf), consultada el 17.06.21

"Estas herramientas están publicadas con la finalidad de ayudar u homogeneizar conceptos en la determinación de si las medidas que se propongan son acordes con la legislación en materia de protección de datos en la Unión Europea. Consideran los redactores que de esa forma contribuyen a una mejor preparación de los decisorias políticos y los legisladores europeos en su misión de preparar y/o examinar propuestas que impliquen el tratamiento de datos personales y limiten derechos y libertades de los reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea".

[274] European Union Agency for Fundamental Rights, "Fundamental Rights Report 2018", ISBN 978-92-9491-928-1 en http://fra.europa.eu/en/publicatin/2018/fundamental-rights-report-2018

la aplicación e interpretación del artículo 8 del CEDH y del artículo 8 de Carta"[275] (Von Hannover contra Alemania, 2012).

Aún con todo lo anterior, los Estados miembros pueden aprobar legislación nacional que permita ajustar el equilibrio en la protección de los datos personales y el ejercicio de otros derechos. En ese sentido, el Reglamento general de protección de datos de la UE prevé excepciones[276].

El SEPD ha observado que, en los últimos años, la protección de los datos personales ha cobrado impulso y se reconoce cada vez más como una dimensión que debe tener en cuenta el legislador en todos los ámbitos políticos y en casi todas las iniciativas de la Comisión. Esto no se debe únicamente a una mayor concienciación del público, sino a la capacidad cada vez mayor del tratamiento de datos (que hasta hace poco parecía inofensivo) de incidir gravemente en la vida de todos y cada uno de los ciudadanos. Por ello, decidió publicar una *"Guía relativa a la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la privacidad y a la protección de los datos personales"*[277] con el mismo propósito que las *"herramientas"* que ya emitió en 2017, es decir, ayudar a evaluar la conformidad de las medidas propuestas con la legislación de la UE en materia de protección de datos y apoyar mejor a los responsables políticos y a los legisladores de la UE encargados de preparar o examinar las medidas que implican el tratamiento de datos personales y limitan los derechos a la protección de los datos personales y a la intimidad para encontrar soluciones que minimicen el conflicto entre estas prioridades y sean proporcionadas. Quizás si esta guía se hubiera publicado en 2006 y se hubiera tenido en cuenta en la negociación de la Directiva de Conservación de Datos, no habría sido declarada nula por el Tribunal europeo. Esta guía es útil y práctica, porque ofrece una

[275] TEDH, Von Hannover contra Alemania (nº 2), números 40660/08 y 60641/08, de 7 de febrero de 2012; TJUE, asuntos acumulados C-468/10 y C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito y Federación de Comercio Electrónico y Marketing Directo contra Administración del Estado, 24 de noviembre de 2011, apartado 48; TJUE, C-275/06, Productores de Música de España contra Telefónica de España SAU, 29 de enero de 2008, apartado 68.

[276] Artículo 23.1 del RGPD de la Unión Europea (DOUE L119/1 de 4.5.2016).

[277] Documento de trabajo del Consejo, nº 7239/19, de 7 de marzo de 2019, por el que se adjunta una carta del SEPD que anuncia el lanzamiento de un procedimiento de consulta sobre el borrador de *"Guía para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la privacidad y a la protección de datos personales"*, en https://delegates.consilium.europa.eu

metodología clara, paso a paso, para evaluar la proporcionalidad ante las nuevas propuestas normativas[278].

Recordemos en este punto el contenido del artículo 52, apartado 1 de la Carta, respecto de los criterios que debe cumplir toda limitación de derechos fundamentales para que sea legal:

- debe estar prevista por la ley,
- debe respetar la esencia de los derechos,
- debe responder realmente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades de los demás,
- debe ser necesaria, y
- debe ser proporcionada.

En primer lugar, debe examinarse si la ley que establece una limitación es accesible y previsible. Si no se cumple este requisito, la medida es ilegal y no es necesario seguir con su análisis. En cuanto al concepto *previsto por la ley,* en virtud del artículo 52, apartado 1 de la Carta, deben utilizarse los criterios desarrollados por el TEDH, tal como se sugiere en varias opiniones de los abogados generales del TJUE[279]. De ahí que pueda hacerse referencia, entre otras, a la sentencia del TEDH en el *caso Weber y Saravia c. Alemania,* párrafo. 84: *"El Tribunal de Justicia reitera que la expresión 'conforme a Derecho' en el sentido del artículo 8, apartado 2, del CEDH exige, en primer lugar, que la medida impugnada tenga algún fundamento en el derecho interno; también se refiere a la calidad del derecho en cuestión, exigiendo que sea accesible a la persona afectada, que, además, debe poder prever sus consecuencias para ella, y compatible con el Estado de Derecho"*. Sobre la noción de *previsibilidad* en el contexto de la interceptación de comunicaciones, el Tribunal europeo ha sostenido en

[278] La guía está basada en estudio de casos del TJUE, del TEDH, Opiniones del SEPD y del Grupo de Trabajo del Artículo 29, además de las instrucciones del Comité Europeo de Protección de Datos.

[279] Ver las opiniones en los asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, párrafos. 137-154 y en el asunto C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, párrafos. 88-114. Ver también el considerando 41 del RGPD: *"Dicha medida legislativa debe ser clara y precisa y su aplicación debe ser previsible para las personas sujetas a ella, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (...) y del Tribunal Europeo de Derechos Humanos"*.

varias ocasiones que no puede ser la misma que en otros ámbitos, que no puede significar que un individuo deba ser capaz de prever cuándo es probable que las autoridades intercepten sus comunicaciones para poder adaptar su conducta en consecuencia, y que existe riesgo de arbitrariedad. Por lo tanto, considera que es esencial contar con normas claras y detalladas sobre la interceptación de las conversaciones telefónicas, especialmente porque la tecnología disponible para su uso es cada vez más sofisticada. El derecho interno debe ser lo suficientemente claro como para dar a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades están facultadas para recurrir a tales medidas[280].

En segundo lugar, si la medida ha superado la prueba de la calidad del derecho, debe examinarse si se respeta la esencia de este, es decir, si el derecho se vacía de hecho de su contenido básico y el individuo no puede ejercerlo. Si la esencia del derecho se ve afectada, la medida es ilegal y no es necesario seguir evaluando su compatibilidad con las normas establecidas en el apartado 1 del artículo 52 de la Carta[281].

En los *asuntos acumulados C-293/12 y C-594/12, Digital Rights, ECLI:EU:C:2014:238 párrafo 39*, el Tribunal de Luxemburgo consideró que la esencia del derecho al respeto de la vida privada no se veía afectada, puesto que la Directiva de conservación de datos no permitía conocer el contenido de las comunicaciones electrónicas sino únicamente los datos de tráfico y de localización [los *metadatos*].

[280] Ver el caso del TEDH, Zakharov c. Rusia, párrafo 229.

[281] Aunque la jurisprudencia no es abundante en lo que respecta a las condiciones en las que se ve afectada la esencia de un derecho, se puede argumentar que sería así si la limitación va tan lejos que vacía el derecho de sus elementos esenciales y, por tanto, impide el ejercicio del derecho.

En el asunto C-362/14, Schrems, ECLI:EU:C:2015:650, párrafos 94 y 95, el TJUE consideró que la esencia del derecho al respeto de la vida privada y el derecho a un recurso efectivo estaban afectados: "una normativa que permite a las autoridades acceder de forma generalizada al contenido de las comunicaciones electrónicas debe considerarse que compromete la esencia del derecho fundamental al respeto de la vida privada, garantizado por el artículo 7 de la Carta (...). Del mismo modo, una legislación que no prevea ninguna posibilidad de que una persona pueda interponer recursos judiciales para acceder a los datos personales que le conciernen, o para obtener la rectificación o la supresión de dichos datos, no respeta la esencia del derecho fundamental a la tutela judicial efectiva, consagrado en el artículo 47 de la Carta" (párrafos 94 y 95). El Tribunal no profundizó en la necesidad de tal limitación, e invalidó -también por otros motivos- la Decisión de la Comisión sobre la adecuación de los principios de puerto seguro.

Consideró igualmente que la esencia del derecho a la protección de los datos personales no se veía afectada porque la Directiva establecía la norma básica respecto a que debían adoptarse medidas organizativas y técnicas apropiadas contra la destrucción, pérdida o alteración accidental o ilícita de los datos conservados[282]. Sólo tras la apreciación de que la esencia del derecho fundamental en juego no estaba comprometida, procedió a examinar la necesidad de la medida.

En los *asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, apartado 123*[283], el Alto Tribunal afirmó que la privación del control por parte de una autoridad independiente del cumplimiento del nivel de protección garantizado por el derecho de la Unión podía afectar también a la esencia del derecho a la protección de los datos personales, ya que así lo exige expresamente el artículo 8, apartado 3, de la Carta, y *"si no fuera así, las personas cuyos datos personales fueran retenidos se verían privadas del derecho, garantizado en el artículo 8, apartados 1 y 3, de la Carta, a presentar ante las autoridades nacionales de control una reclamación solicitando la protección de sus datos"*.

En tercer lugar, hay que examinar si la medida responde a un objetivo de interés general. El objetivo de interés general proporciona el contexto en el que se puede evaluar la necesidad de la medida. Este se debe examinar con suficiente detalle para ver que se cumple este criterio.

En cuarto lugar, evaluar la necesidad de una medida legislativa propuesta que implique el tratamiento de datos personales; lo que se denomina *"prueba de necesidad"*. Esta prueba conlleva una evaluación combinada, basada en hechos, de la eficacia de la medida para el objetivo perseguido y de si es menos intrusiva en comparación con otras opciones para lograr el mismo objetivo.

[282] TJUE Sentencia de 8 de abril de 2014, *Caso Digital Rights*, apartados 39 y 40.
[283] TJUE Sentencia de 21 de diciembre de 2016, *Caso Tele 2 Sverige AB*, apartado 123.

La necesidad es también un principio de calidad de los datos y una condición recurrente en casi todos los requisitos sobre la legalidad del tratamiento de los datos personales que nacen del Derecho derivado de la protección de datos de la Unión Europea. Solo una medida que se demuestre necesaria debe someterse a la prueba de proporcionalidad. En casos recientes, el TJUE no ha procedido a evaluar la proporcionalidad tras considerar que las limitaciones a los derechos de los artículos 7 y 8 de la Carta no eran estrictamente necesarias. Por ejemplo, una medida de aplicación de la ley, si se considera necesaria, debe analizarse en función de si fuese más proporcionada si se limitara únicamente a los delitos graves. Una prueba de proporcionalidad podría implicar la evaluación de las reglas que deberían acompañar a una medida de vigilancia antes o después de su autorización: dichas pautas, a menudo denominadas *"salvaguardias"*, servirán para reducir los riesgos para los derechos fundamentales que plantea la medida prevista.

En la práctica, un aspecto específico o una disposición contenida en un proyecto de medida pueden ser relevantes tanto para la evaluación de la necesidad como de la proporcionalidad. Por ejemplo, la cuestión de si una medida debe dirigirse a cualquier delito o sólo a los delitos graves puede considerarse una cuestión de necesidad; sin embargo, si se considera que dicha disposición es necesaria, aún sería preceptivo evaluar su proporcionalidad y su riesgo de erosión de los valores de una sociedad democrática. En definitiva, por tanto, existe un cierto solapamiento entre las nociones de necesidad y proporcionalidad, y dependiendo de la medida en cuestión las dos pruebas pueden llevarse a cabo simultáneamente o incluso en orden inverso.

En quinto lugar, si se cumple esta prueba, debe examinarse la proporcionalidad de la medida prevista, que se conoce como *"prueba de proporcionalidad"*. El concepto de proporcionalidad es un concepto jurídico bien establecido en el Derecho de la Unión Europea[284]. *Se* trata de un principio general que exige que *"el contenido y la forma de la acción de la Unión no excedan de lo necesario para alcanzar los objetivos de los Tratados"*.

[284] Artículo 5.4 del TUE.

En virtud del tantas veces mencionado artículo 52, apartado 1 de la Carta, *"sin perjuicio del principio de proporcionalidad, las limitaciones [al ejercicio de los derechos fundamentales] sólo podrán hacerse si son necesarias (...)"*. Según una jurisprudencia reiterada del TJUE, *"el principio de proporcionalidad exige que los actos de las instituciones de la UE sean apropiados para alcanzar los objetivos legítimos perseguidos por la legislación en cuestión y que no excedan los límites de lo que es apropiado y necesario para alcanzar dichos objetivos"*[285]. Por lo tanto, la proporcionalidad en sentido amplio, tal como la denomina el TJUE, abarca tanto la necesidad como la adecuación -proporcionalidad en sentido estricto- de una medida, es decir, la forma y el grado en que existe un vínculo lógico entre y el objetivo [legítimo] perseguido. Para ello, las ventajas resultantes con la adopción de esas acciones no deben ser superadas por las desventajas que provocan con respecto al ejercicio de los derechos fundamentales y, cuando haya que elegir entre unas u otras medidas, tendrá que optarse por la menos lesiva de derechos. Por lo tanto, *"establece límites a las autoridades [en este caso, las agencias encargadas de la aplicación de la ley y otras autoridades administrativas en determinados Estados miembros] en el ejercicio de sus competencias al exigir que se establezca un equilibrio entre los medios utilizados y el objetivo previsto (o el resultado alcanzado o perseguido)"*[286].

De hecho, en la sentencia sobre los derechos digitales[287], el TJUE ha dictaminado que el poder discrecional del legislador se reduce al restringir los derechos fundamentales:

> *"cuando se trata de injerencias en los derechos fundamentales, el alcance de la facultad de apreciación del legislador de la UE puede resultar limitado, en función de una serie de factores, entre los que figuran, en particular, el ámbito*

[285] Asunto C-62/14, Gauweiler (OMT), ECLI:EU:C:2015:400, párrafo. 67. Ver también C-331/88, Fedesa y otros, ECLI:EU:C:1990:391, párrafo. 13: *"En cuanto al control de la proporcionalidad, el principio de proporcionalidad, que es uno de los principios generales del Derecho comunitario, exige que las medidas adoptadas por las instituciones comunitarias no sobrepasen los límites de lo que es apropiado y necesario para alcanzar los objetivos legítimamente perseguidos por la legislación en cuestión; cuando haya que elegir entre varias medidas apropiadas se debe recurrir a la menos onerosa, y los inconvenientes causados no deben ser desproporcionados con respecto a los objetivos perseguidos."*

[286] K. LENAERTS, P. VAN NUFFEL, *European Union Law*, Sweet and Maxwell, 3ª edición, Londres, 2011, p. 141 (asunto C-343/09, Afton Chemical, párr. 45; asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke y Hartmut Eifert, ECLI:EU:C:2010:662, párrafo. 74; asuntos C-581/10 y C-629/10, Nelson y otros, párrafos. 71; asunto C-283/11, Sky Österreich, párrafo. 50; y asunto C-101/12, Schaible, párrafo. 29).

[287] Asuntos acumulados C-293/12 y C-594/12, ECLI:EU:C:2014:238.

de que se trate, la naturaleza del derecho en cuestión garantizado por la Carta, la naturaleza y la gravedad de la injerencia y el objeto perseguido por "[288].

En esencia, ante la pregunta *"¿Cuál es el alcance de la discrecionalidad (reducida) del legislador de la Unión Europea?",* el Alto Tribunal declaró que la legislación europea debe concretar las medidas de forma clara y precisa en la regulación del alcance de s y con unas garantías *"mínimas"* para los afectados [los propietarios de los datos], de tal forma que s *"tengan una composición suficiente de tres pasos: (i) adecuación; (ii) necesidad; y (iii) proporcionalidad stricto sensu"*[289].

Respecto de la relación entre proporcionalidad y necesidad, también en este caso se debe hacer una evaluación conjunta y combinada de ambos principios [basada en hechos] respecto de la eficacia de las medidas establecidas en el cumplimiento del objetivo perseguido y de si es menos intrusiva en comparación con otras opciones para lograr el mismo objetivo. La prueba de necesidad debe considerarse como el primer paso sobre una medida que implique el tratamiento de datos personales. Si el proyecto de medida no supera la prueba de necesidad, no es necesario examinar su proporcionalidad. Una medida que no se demuestre que es necesaria, considera el Supervisor Europeo de Protección de Datos que no debería proponerse a menos que y hasta que se haya modificado para cumplir el requisito de necesidad; en otras palabras, la necesidad sería una condición previa y sine qua non a la proporcionalidad[290]. Como referimos anteriormente, en algunos casos recientes el Tribunal incluso no procedió a evaluar la proporcionalidad tras considerar que las limitaciones a los derechos de los artículos 7 y 8 de la Carta no eran estrictamente necesarias[291].

[288] *Ibíd*. apartado 47.

[289] Para ampliar, vid. C. BAGGER TRANBERG, C. *"Proporcionalidad y protección de datos en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas"*, International Data Privacy Law, 2011, Vol. 1, nº 4, pina 240.

[290] En los asuntos acumulados C-465/00, C-138/01y C-139/01, Rechnungshof, ECLI:EU:C:2003:294 párrafo. 91 , el TJUE sostuvo que *"Si los tribunales nacionales llegan a la conclusión de que la legislación nacional controvertida es incompatible con el artículo 8 del Convenio, dicha legislación tampoco puede satisfacer el requisito de proporcionalidad de los artículos 6, apartado 1, letra c), y 7, letras c) o e), de la Directiva 95/46"*.

[291] Sentencia TJUE caso C-362/14, Schrems, ECLI:EU:C:2015:650.

1. Principio de proporcionalidad en la Directiva 2006/24/CE

El principio de proporcionalidad respecto de la conservación de datos y su posterior cesión ha ido evolucionando a lo largo del tiempo y la jurisprudencia del TJUE ha ido configurando cómo debemos interpretarla respecto de la labor de investigación, persecución del delito y su enjuiciamiento. Recoge Pesqueira Zamora (2020; 438)[292] tres sentencias del Tribunal de Luxemburgo al respecto:

- La primera es la ya conocida Sentencia del *Caso Digital Rights*, cuyos elementos principales veremos a continuación.
- La segunda corresponde a la Sentencia de 21 de diciembre de 2016, en los *casos acumulados C-203/15 y C-698/15*, que valoró la idoneidad de las normativas nacionales de transposición de la Directiva anulada. En este caso, que también analizaremos más adelante, es importante destacar el principio de especialidad, que exige que una medida esté relacionada con la investigación de un delito concreto, lo que impide la adopción de medidas de investigación mediante la conservación y acceso a los datos de operadores tecnológicos al objeto de prevenir delitos.
- La tercera se deriva de la cuestión prejudicial en el *Caso C-207/16*, relativa a la gravedad del delito como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta. Precisamente, en la Sentencia *Digital Rights*, apartado 46, el Tribunal reafirmó que la proporcionalidad se compone de los pasos de adecuación y necesidad y estableció que la limitación con los derechos protegidos en los artículos 7 y 8 de la Carta no era necesaria (apartado 65) y, por tanto, concluyó que las limitaciones no eran proporcionadas (apartado 69).

Empero, como hemos resaltado antes, una vez que se considera que una medida legislativa es necesaria, debe examinarse en función de su proporcionalidad. Una prueba de proporcionalidad implica la evaluación de las *salvaguardias* que deben acompañar a esta[293] con el fin de reducir los riesgos planteados por la medida prevista para los derechos y las libertades fundamentales de las personas afectadas, a un nivel

[292] PESQUEIRA ZAMORA, M.J., *"Diligencias de investigación, cesión de datos y principio de proporcionalidad"*, Universidad Abat Oliba, InDret, 2020, pp. 419-445, p. 438.

[293] Por ejemplo, en materia de vigilancia.

aceptable/proporcionado. Otro factor que debe tenerse en cuenta en la evaluación de la proporcionalidad es la eficacia de las medidas existentes por encima de las propuestas. En definitiva, la evaluación deberá ser efectuada necesariamente caso por caso por el legislador a la hora de aprobar medidas de limitación de derechos.

Según Bygrave (2014; 147), la *"aparición de un requisito de proporcionalidad"* se ha considerado *"uno de los avances más sorprendentes de la última década en la legislación europea sobre la privacidad de los datos"*[294].

Para el Supervisor Europeo de Protección de Datos, en el núcleo de la noción de proporcionalidad se encuentra el concepto de *"ejercicio de equilibrio"*: la ponderación de la intensidad de la interferencia frente a la importancia del objetivo alcanzado en el contexto dado. Para ser completa y precisa, una prueba bien realizada necesita la identificación expresa, y la estructuración en un marco coherente, de los diferentes elementos de los que depende la ponderación. Por lo tanto, la claridad de la medida que restringe los derechos fundamentales a la intimidad y/o a la protección de datos es una condición previa para la identificación de la intensidad de la interferencia. Esta última, a su vez, es necesaria para verificar si la repercusión sobre estos derechos fundamentales es proporcionada al objetivo perseguido por la legislación examinada.

El TJUE también considera que la proporcionalidad implica una apreciación caso por caso:

> *"Corresponde al órgano jurisdiccional remitente tener en cuenta, con arreglo al principio de proporcionalidad, todas las circunstancias del asunto del que conoce, en particular la duración de la infracción de las normas de aplicación de la Directiva 95/46 y la importancia para las personas afectadas de la protección de los datos divulgados"*[295].

[294] BYGRAVE, L.A., *"Data Privacy Law. An International Perspective"*, Oxford University Press, 2014, p. 147.

[295] Sentencia TJUE, caso C-101/01, Linqvist, ECLI:EU:C:2003:596, párrafo 89.

De forma práctica, en este caso también ha querido el Supervisor Europeo de Protección de Datos facilitar la labor de los decisorios políticos y armonizar la forma de actuar, para evitar futuras sentencias que invaliden todo el largo y difícil proceso que se ha de seguir para adoptar una norma legislativa europea. En ese sentido, ha publicado en su guía[296] recomendaciones dirigidas al legislador a la hora de evaluar la necesidad y la proporcionalidad:

1) En cuanto a la prueba de necesidad[297]:

- El *paso 1* requiere una descripción fáctica detallada de la medida propuesta y de su finalidad, antes de cualquier otra evaluación.
- El *paso 2* ayuda a identificar si la medida propuesta representa una limitación del derecho a la protección de los datos personales o del respeto a la vida privada, y posiblemente también de otros derechos.
- El *paso 3* examina el objetivo de la medida con respecto al cual debe evaluarse su necesidad.
- El *paso 4* ofrece orientación sobre los aspectos específicos que deben abordarse al realizar la prueba de necesidad, en particular que la medida debe ser eficaz y lo menos intrusiva posible.

Si la evaluación de la medida lleva a la conclusión de que cumple el requisito de necesidad (prueba 1), puede examinarse según los siguientes pasos correspondientes a la prueba de proporcionalidad (prueba 2). Es decir, si se considera que ha superado la prueba 1, significa que se trata de la medida efectiva menos intrusiva disponible para alcanzar el objetivo perseguido y se evalúa ahora si la limitación (interferencia) que provoca es proporcionada al objetivo que se pretende alcanzar.

2) En cuanto a la proporcionalidad:

- El *paso 1* evalúa la importancia *(legitimidad*) del objetivo y si la medida propuesta cumpliría este objetivo, y aborda la cuestión identificada en la

[296] Guía de Necesidades del SEPD, en https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en .

[297] Vid. p. 9 de la Guía de Necesidades del SEPD.

definición del problema *(cumple realmente*) y en qué medida (en términos de *ventaja/beneficio*).

- El *paso 2* evalúa el alcance, la extensión y la intensidad de la interferencia en términos de impacto sobre los derechos fundamentales a la privacidad y a la protección de datos (en términos de *desventaja/el coste*).
- El *paso 3* evalúa el equilibrio justo (*ventaja/desventaja; beneficio/coste*) de la medida.
- El *paso 4* toma una decisión (*seguir/no seguir*) sobre la medida. Si el resultado es negativo, teniendo en cuenta todos los factores que determinaron la evaluación como desproporcionada, habrá que identificar e introducir salvaguardias que puedan hacer que la medida sea proporcionada.

Antes de llegar a estas sentencias, el TJUE dictó otra también sobre la Directiva de Conservación de Datos, esta vez en el *caso C-301/06, Ireland v. European Parliament and Council of the European Union, ECLI:EU:C:2009:68, 10 de febrero 2009*[298]. El Abogado General Y. Bot opinó en sus Conclusiones que había dos cuestiones fundamentales que la sentencia debía tener en cuenta: si las medidas que preveía la norma europea eran adecuadas a la finalidad perseguida y si eran necesarias para alcanzar esos fines o había otras alternativas menos lesivas con los derechos afectados. En ese caso, como también en las sentencias que analizaremos con más profundidad, la primera cuestión fue respondida afirmativamente, es decir, la Directiva preveía medidas adecuadas para la investigación, detección y enjuiciamiento de delitos graves, de acuerdo con la definición que cada Estado miembro otorga a ese concepto. A juicio de parte de los expertos, más discutible fue el cumplimiento del requisito de necesidad, puesto que las medidas adoptadas debían ser realizables y eficaces para alcanzar los fines propuestos y, al mismo tiempo, las menos invasivas de las disponibles en los derechos afectados. El Tribunal de Justicia señaló que la Directiva regulaba la obligación de conservar los datos de telecomunicaciones, pero no regulaba el acceso o el uso de esos datos por parte de los Estados miembros en el marco de la aplicación de la Directiva. Sin embargo, como señaló el TJUE, el recurso interpuesto por Irlanda se refería únicamente a la elección de las bases jurídicas, y no a una posible vulneración de

[298] Sentencia TJUE (Gran Sala), de 10 de febrero de 2009, en el asunto C-301/06, Ireland contra Parlamento Europeo y Consejo de la Unión Europea.

los derechos fundamentales derivada de la interferencia con el ejercicio del derecho a la intimidad recogido en la Directiva de conservación de datos. En otras palabras, el Tribunal no podría haber abordado la cuestión de la vulneración de los derechos fundamentales, puesto esto habría supuesto ir más allá de los límites de la cuestión planteada.

Por otro lado, en el informe de la Comisión que acompañaba a la propuesta de Directiva se argumentaba que su propuesta cumplía con el principio de proporcionalidad ya que, como reza en la Exposición de Motivos: *"su impacto sobre los ciudadanos y la industria se había limitado al máximo"*, pues consideraba que solo abarcaba a los datos de tráfico, quedando fuera el contenido de las comunicaciones[299]. Además, continuaba defendiendo que la propuesta buscaba el equilibrio entre los intereses en juego y los derechos de los afectados, entre ellos, los requisitos de seguridad e intimidad. De forma particular, la evaluación de la proporcionalidad se había extendido a las categorías de datos afectados por la medida de conservación y el período de retención. Sin embargo, el SEPD fijaba en su dictamen lo que a su entender debían ser los requisitos para valorar en el juicio de proporcionalidad y consideraba que no se cumplían:

- Los plazos debían estar alineados con las necesidades reales de las agencias de aplicación de la ley,
- La cantidad de datos también debía ser realista de acuerdo con las necesidades policiales,
- Debían evitarse los accesos y el uso por personas ajenas a las legalmente determinadas para ello, mediante el establecimiento de medidas de seguridad adecuadas.
- Pasado el plazo de conservación establecido, debía garantizarse su borrado, para lo que se debían establecer medidas de seguridad y organizativas adecuadas.

Aun así, en la sentencia de 2009, el Tribunal confirmó la Directiva de Conservación de Datos, aunque, como reseñábamos antes, no entró en el fondo de las

[299] Exposición de Motivos de la Propuesta COM de 21 de septiembre de 2005, p. 7

cuestiones que el Comité Económico y Social y el GT29 pusieron sobre la mesa, por cuanto lo que se le había planteado fue que la Directiva 2006/24/CE no se había adoptado sobre la base jurídica apropiada (Irlanda consideraba que la elección del artículo 95 CE[300] como base jurídica era inapropiada e injustificable, puesto que la Directiva estaba claramente orientada hacia la represión de las infracciones penales, mientras que, según este Estado miembro, las medidas que se adopten en base al artículo 95 CE debe tener como objetivo central la aproximación de las legislaciones nacionales con objeto de mejorar el funcionamiento del mercado interior y no la represión de las infracciones penales. Este litigio se centraba fundamentalmente en lo que hemos venido analizando respecto del ámbito competencial correspondiente al Primer o Tercer pilar que sustentaba la estructura comunitaria antes del Tratado de Lisboa.

De acuerdo con la jurisprudencia que hemos venido citando, en la parte correspondiente a la prueba de proporcionalidad, en el *Caso Digital Rights Ireland* se consideró quebrada la última de las pruebas, dado que el sistema de conservación de datos no cumplía con ciertas salvaguardas mínimas, como los límites de aplicación, la intervención de autoridades nacionales de control, la imposición de un periodo de tiempo reducido para la conservación de datos y la posibilidad de ejercicio de un recurso efectivo[301]. También en este caso, lo citamos otra vez [en esta ocasión de forma específica] literalmente: *"el principio de proporcionalidad exige que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos"*[302] (Sentencia Digital Rights, 2014; apartado 46).

Un ejemplo concreto que tiene similitudes con la cuestión planteada por Irlanda lo encontramos [por no hacer referencia solo a España cuando se desciende al nivel nacional] en Alemania con algunas de las leyes que promulgó este país para hacer frente a la amenaza terrorista: las leyes sobre cotejo de matrículas en determinados Länder,

[300] Artículo 114 del TFUE.
[301] Sentencia TJUE, Caso Digital Rights Ireland, Cf. 45-66.
[302] Sentencia TJUE, Caso Digital Rights Ireland, Cf.,46.

que preveían el almacenamiento de números de matrículas seleccionados arbitrariamente, mediante grabación con cámaras de los vehículos que circulaban por las carreteras y su posterior almacenamiento por la Policía. El Tribunal Federal Alemán consideró que estos datos no eran inocuos en sí mismos y su tratamiento podía lesionar derechos de los ciudadanos. Apuntó una reflexión interesante que puede servir también para el caso de la Directiva europea [lo consideramos más adelante], cual es: *"no habría amenaza al derecho si fueran anónimos durante todo el proceso y, además, se destruyesen una vez se contrastasen las matrículas con los ficheros policiales…[…], pero en el momento en que se produce la coincidencia entre el fichero y el número de matrícula, comienza un peligro concreto para la libertad de acción y la privacidad de la persona, que el derecho de autodeterminación informativa protege"*[303]. En este caso, el Tribunal federal siguió el mismo razonamiento que el Alto Tribunal: determinó la importancia de la injerencia en el derecho afectado y, a continuación, comprobó el respeto al principio de proporcionalidad (además del de reserva de ley). Respecto del respeto al principio de proporcionalidad, consideró que las medidas adoptadas con la recogida y cotejo de matrículas cumplían de forma adecuada con el fin pretendido, pero no guardaban proporción con el bien que quería proteger. En ese sentido, el Tribunal hace una reflexión que encontramos muy pertinente traer a este estudio:

> *"la prohibición de injerencias desproporcionadas en los derechos es un límite al deber del Estado de proteger otros bienes jurídicos. La vida, la integridad física de las personas o las amenazas a la existencia del Estado, son bienes de especial trascendencia, pero su protección no justifica una medida que ponga en juego la personalidad de los afectados sin una situación de clara amenaza"*[304].

Explica González Pascual (2009; 952),[305] a colación de la reflexión anterior, la Sentencia de 4 de abril de 2006 del Tribunal alemán que afirmaba que *"ni la situación internacional generada tras el 11-S, ni las tensiones en las relaciones internacionales justifican medidas antiterroristas que impliquen una intensa injerencia en los derechos fundamentales"*. En este y otros casos similares, el Tribunal alemán exige equilibrio

[303] BVerfG, 1 BvR 2074/05 vom 11.3.2008, párrafos 68 y 69.
[304] BVerfG, 1 BvR 370/07, vom 27.2.2008, párrafos 247-248.
[305] GONZÁLEZ PASCUAL, M.I., *"El Tribunal Constitucional Federal alemán ante la compatibilidad con los derechos fundamentales de la normativa nacional de origen europeo de prevención de delitos"*, en Revista de Derecho Comunitario Europeo, ISSN 1138-4026, nº. 34, Madrid, septiembre/diciembre, 2009, pp. 945-966, pp. 952.

entre la seguridad y la libertad sin sobrepasar los límites que lleven a una injerencia no acorde con el derecho alemán. Podríamos extrapolar esta conclusión a aquella a la que el Tribunal europeo de Luxemburgo llegó en el estudio de la Directiva europea de Conservación de Datos.

En el apartado 51 de la *Sentencia Digital Rights Ireland*, se reconoce que:

> *"en cuanto al carácter necesario de la conservación de datos que impone la Directiva 2006/24/CE, ha de señalarse que es cierto que la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación. Sin embargo, este objetivo de interés general, por fundamental que sea, no puede por sí solo justificar que una medida de conservación como la establecida en la Directiva 2006/24/CE se considere necesaria a los efectos de dicha lucha"*[306].

En definitiva, se considera que no se ha cumplido con el criterio de necesidad para alcanzar el objetivo perseguido.

No hay consenso tampoco entre los expertos respecto de esta cuestión, de forma que algunos autores, como Fernández Rodríguez (2016; 109)[307], sostienen que el Tribunal no usa de forma rigurosa el principio de proporcionalidad en sus diversos aspectos o escalones en la Sentencia Digital Rights.

1.1 Conjunto de datos a conservar

En el anexo de la propuesta de Directiva se reflejaban las categorías de datos que serían retenidos (datos de tráfico y de localización/metadatos):

[306] Sentencia TJUE Caso Digital Rights Ireland, Cf. Apartado 51.

[307] FERNÁNDEZ RODRÍGUEZ, J.L., *"Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente"*, en Centro de Estudios Políticos y Constitucionales, Revista Española de Derecho Constitucional, nº. 108 (septiembre/diciembre 2016), p. 109.

- *Datos necesarios para rastrear e identificar el origen de una comunicación.*
- *Datos necesarios para identificar el destino de una comunicación.*
- *Datos necesarios para identificar la fecha, hora y duración de una comunicación.*
- *Datos necesarios para identificar el tipo de comunicación.*
- *Datos necesarios para identificar el equipo de comunicación de los usuarios.*
- *Datos necesarios para identificar la localización del equipo de comunicación móvil*

La aprobación del expediente legislativo, como es habitual, suscitó diferencias de parecer sobres cuestiones técnicas concretas: nos referimos en particular a la consideración que debía darse a las llamadas perdidas y si la localización de la llamada debía serlo solo al inicio o durante toda la conversación. El Comité Económico y Social y el GT29 se pronunciaron a favor de la opción más restrictiva y, en consecuencia, menos lesiva con los derechos de los ciudadanos, pero el texto final incorporó las demandas de los servicios policiales, puesto que permitía un mayor control sobre los movimientos de los investigados.

1.2 Período de conservación de los datos

Respecto del periodo adecuado de conservación de los datos, para garantizar la eficacia de la medida y, al mismo tiempo, limitar la intromisión en el derecho a la protección de estos, la Directiva no diferenció entre periodos distintos dependiendo del tipo de datos ni del tipo de delito grave a cuya investigación o enjuiciamiento serviría. A pesar de la evaluación de impacto que acompaña a toda propuesta legislativa que realiza la Comisión, es difícil pensar, de acuerdo con el proceso de elaboración y aprobación de normas en la Unión, que se contara con datos fiables proporcionados por las diferentes partes interesadas *(stakeholders)* ni antes ni durante la negociación de los textos, por lo que es muy probable que no se pudieran determinar con rigor si seis meses, un año o dos años son los periodos necesarios. La experiencia en este tipo de negociaciones en las instituciones europeas indica que el consenso se alcanza en el periodo intermedio respecto del que inicialmente propone la Comisión -mínimo que

suele aceptar como el Consejo- y lo que defiende el Parlamento. En este caso, la propuesta inicial era de uno a tres años y finalmente se adoptó una franja entre seis meses y dos años. Otra práctica habitual en los primeros momentos del inicio de las discusiones en un expediente legislativo es que, cuando no hay datos concretos que se consideran necesarios para tomar una decisión y se pide opinión o la aportación de esos datos a algunas de las partes interesadas (en este caso a los servicios policiales) aquel Estado miembro que dispone de ellos y los presenta y los defiende, suele condicionar al resto. Y eso es lo que, según apunta Rodríguez García (2013; 246), ocurrió con la propuesta de Directiva de Conservación de Datos[308]. En este caso, apunta el autor, el Supervisor Europeo de Protección de Datos no se mostró conforme con las cifras presentadas, argumentando que *"el hecho de que en algunos casos la disponibilidad de datos del tráfico y/o de localización ayudara a resolver el delito no significa automáticamente que esos datos sean necesarios, en general, como instrumento para los servicios policiales"*. En un estudio reciente elaborado a propuesta de la Comisión, que veremos más adelante, una vez dictadas las sentencias del Alto Tribunal sobre la invalidación de la Directiva, se aportan datos más concretos y variados sobre la importancia del periodo de conservación de los datos para las investigaciones de los servicios policiales y la persecución de delitos. El Grupo del Artículo 29 tampoco apoyaba la propuesta de la Comisión respecto de los plazos de conservación y así lo puso de manifiesto.

1.3 Conservación generalizada de los datos

Esta es una cuestión fundamental que ya desde el comienzo fue controvertida y posteriormente se convirtió en un elemento central de la discusión jurídica respecto de la validez o invalidez de la Directiva. Quienes cuestionaron el propósito de la Directiva, acertaron. Una vez más, reiteramos que el Grupo del Artículo 29 tampoco estaba de acuerdo con la conservación generalizada de todos los datos, puesto que no se aportaba prueba que justificara esa necesidad a efectos de orden público. Estos argumentos no se

[308] RODRÍGUEZ GARCÍA, L.F., *"La Directiva europea sobre Conservación sobre…."*, p. 246. *"Durante la elaboración de la DCD, tanto la Comisión como la Presidencia del Consejo concedieron importancia a un estudio de la Policía del Reino Unido que demostraba que, aunque el 85% de los datos de tráfico requeridos por la Policía tenían un máximo de seis meses de antigüedad, en tanto que los datos de entre seis meses y un año se utilizaban en investigaciones complejas de delitos más graves"*.

plantearon respecto de la propuesta de Directiva sino para la Decisión Marco[309] anterior, que no vio la luz; por lo tanto, esos mismos argumentos se reprodujeron después respecto del borrador de Directiva. Otro argumento desfavorable del Supervisor Europeo de Protección de Datos estaba relacionado con determinados servicios que, si bien su conservación no aportaba beneficio alguno a los proveedores de servicios[310], por cuanto no afectaban a su facturación, sí eran considerados de interés por los servicios policiales; en consecuencia, su conservación excedía del propósito por el que los operadores de servicios podían retenerlos, según la Directiva de privacidad electrónica.

Ya se cuestionó también en ese momento uno de los argumentos que todavía hoy utilizan los servicios policiales para justificar la necesidad de adoptar medidas: que la evolución tecnológica hacía necesario disponer de herramientas que, con respeto a la protección de datos, permitieran estar a la altura de los avances tecnológicos en la lucha contra la delincuencia grave y el enjuiciamiento de los autores. El Dictamen del Grupo del Artículo 29 cuestionaba que la necesidad implicara la conservación de todos los datos de todos los usuarios y no se utilizaran otros medios igualmente útiles y menos lesivos de derechos, como el procedimiento de congelación rápida -*quick freeze*-, del que hablaremos más adelante. No obstante, si bien este método de conservación y acceso puede ser viable para determinadas investigaciones, no lo es para aquellas que precisan del acceso al histórico de datos: aquellos datos anteriores al momento en el que se conocen los hechos o son denunciados por la víctima, o para investigaciones que son especialmente complejas y duraderas en el tiempo, como las de terrorismo o delincuencia organizada transnacional.

[309] 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 el suministro de datos en redes públicas de comunicaciones a efectos de la prevención, investigación, descubrimiento y represión de la delincuencia y de las infracciones penales, con inclusión del terrorismo, presentada por la República Frances, Irlanda, el Reino Unido y el Reino de Suecia, el 28 de abril de 2004 (CNS/2004/0813), en http://register.consilium.eu/int/pdf/es/04/st08/st08958.es04.pdf

[310] Servicios como los de las tarjetas prepago o suscripciones a tarifas planas.

CAPÍTULO VI. CONTEXTO LEGAL Y POLÍTICO SOBRE LA CONSERVACIÓN DE METADATOS. DEL CASO DIGITAL RIGHTS IRELAND HASTA HOY

El incremento del uso de las redes de comunicación -que se hace también extensiva a nuevas formas delictivas- para las actividades cotidianas de los ciudadanos y las transacciones diarias de las empresas, como se ha mencionado ya anteriormente, ha proporcionado información muy valiosa a las empresas de servicios de telecomunicaciones e información (metadatos, que se complementan con la información que permite identificar al subscriptor[311] del servicio).

Esta información solo puede ser utilizada por el operador para fines comerciales: facturación y otras actividades de prestación del servicio; pero, con el consentimiento de los titulares de los datos, pueden ser puestos a disposición de otros prestadores de servicios adicionales, como aplicaciones que permiten posicionar al usuario y ofrecerle con precisión un determinado servicio en el lugar en el que en ese momento se encuentre o incluso llegar a saber sus preferencias por un determinado producto y poder enviarle información comercial personalizada, o aportarle información comercial también de otros productos relacionados con uno en concreto e influir así en sus gustos o preferencias de consumo, etcétera.

Es cierto que el valor de esa información para las autoridades encargadas de hacer cumplir la ley radica en su potencial para establecer vínculos entre sospechosos y fijar patrones de comunicación entre diferentes personas, pero constituyen también una importante ayuda en la localización de víctimas o pistas sobre el escenario de un delito o incluso también para descartar la participación de posibles autores en el transcurso de una investigación.

No obstante, los datos conservados exclusivamente con fines comerciales pueden no ser suficientes para garantizar que estas autoridades policiales y judiciales dispongan efectivamente de la información necesaria para llevar a cabo las

[311] Información de abonado.

investigaciones o el enjuiciamiento de un determinado delito, puesto que las necesidades derivadas de la actividad comercial de una empresa de telecomunicaciones no garantizan que se conserven determinados datos también disponibles; ni permiten prever, en caso de que se conserven, que el período de tiempo de conservación sea adecuado a esos mismos fines de investigación penal.

A estas alturas hemos llegado ya a la conclusión de que combatir la delincuencia es un objetivo general para mantener la seguridad y el orden públicos. Por consiguiente, a la vista de las exigencias que establece la normativa europea e internacional y los criterios fijados por el TEDH y el TJUE, es imprescindible que las medidas que se adopten, y de forma particular respecto del aprovechamiento de la información a la que nos venimos refiriendo, establecer obligaciones proporcionadas, necesarias y transparentes de conservación de datos dirigidas a los operadores, a fin de satisfacer las necesidades operativas de los servicios policiales y las autoridades judiciales. Indudablemente, siempre y cuando se establezcan garantías y salvaguardias suficientes para asegurar el cumplimiento estricto de los fines para los que esas medidas se han establecido [ya analizadas en el capítulo anterior]. De acuerdo con la tesis que sostiene Ortiz-Pradillo (2020; 4)[312]:

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

En un primer momento, como hemos visto, el Consejo de la Unión Europea propuso un proyecto de decisión marco sobre esta misma materia sobre la base de los

[312] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas"*, en Revista General de Derecho Procesal, 52, 2020, pp. 1-28, p. 4.

poderes de cooperación policial de la Unión, que recogía la misma obligación de conservación de metadatos a los proveedores de servicios de telecomunicaciones que la que después se incluyó en la Directiva. Sin embargo, la oposición o reticencias del Parlamento Europeo y de las autoridades en materia de protección de datos, precisamente porque adolecía de falta de proporcionalidad, hicieron que se retirara la propuesta. De hecho, para la propuesta de Directiva, hemos ya puesto de relieve el rechazo que, también desde el principio, se suscitó entre expertos en la materia y diversas voces autorizadas, que consideraban que el sistema de conservación de datos y su tratamiento podía hacer pensar que tarde o temprano sería necesaria una reforma para adecuarla a la realidad que esos expertos e instituciones veían venir. Aun así, pasaron ocho años hasta que el Tribunal europeo declaró su invalidez por permitir una injerencia desproporcionada en los derechos, que ya tantas veces hemos citado: *"mientras que la conservación de datos cumple con su objetivo general en interés de la lucha contra el delito grave, la norma no pasaba la prueba de proporcionalidad, puesto que la injerencia en determinados derechos fundamentales no está limitada a lo estrictamente necesario"*, bajo argumentos de que la Directiva no establecía de forma clara y precisa unas reglas concretas en relación con el alcance y la injerencia en los derechos a la privacidad y a la protección de los datos personales que reconoce la Carta de los Derechos Fundamentales de la Unión Europea, además de la falta de suficientes procedimientos de salvaguarda de la protección física de los datos y del acceso indebido por parte de personas o instituciones no habilitadas a tal fin.

Antes de la Directiva, los Estados miembros habían introducido medidas obligatorias respecto de la conservación de metadatos de comunicaciones electrónicas a los efectos de las necesidades de investigación de autoridades policiales y judiciales. Dado que estos enfoques fueron diferentes en unos y otros países, se hizo necesaria la armonización en toda la Unión[313].

[313] Propuesta de la Comisión para una Directiva del Parlamento Europeo y del Consejo sobre la retención de información procesada en relación con la provisión de los servicios de comunicación electrónica pública y por la que se modifica la Directiva 2002/58/EC, COM (2005) 438 final, 21 de septiembre de 2005, disponible en: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2005/0438/COM_COM(2005)0438_EN.pdf, consultada el 02.05.21

La Directiva introdujo una obligación general de retener ciertas categorías de datos procedentes de todos los usuarios, con el propósito de la lucha contra el delito grave, según fuera definido este por cada Estado miembro en su normativa nacional[314]. Obligaba a los proveedores de servicios a retener la información por un período entre seis y veinticuatro meses, en aras a asegurar que estuviera disponible para la investigación, detección y persecución del delito grave. Los proveedores fueron obligados también a poner esa información a disposición de las agencias encargadas de hacer cumplir la ley cuando fuera solicitada. Sin embargo, no se especificaba cómo se accedería a la información ni cómo sería usada por las autoridades competentes. Con esa obligación, los proveedores de servicios intervenían/interferían sobre los derechos de los ciudadanos en cumplimiento de una obligación legal impuesta por la norma europea. Además, se les obligaba a establecer una serie de medidas que permitieran garantizar la seguridad de los datos conservados[315].

Considera González Pascual (2014; 947)[316] que esta obligación constituyó una muestra de *"solapamiento parcial"* de los derechos a la privacidad, por cuanto eran *"más que datos personales"* al referirse *"esencialmente a la vida privada, al secreto de la vida privada, incluida la intimidad"*[317]. Además, afectaba también a la protección de los datos personales, ya que estos serían objeto de tratamiento posterior por los servicios policiales.

[314] En el artículo 1, relativo al objeto, se proponía: *"armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro"*. Se aplicaba *"a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas"* (Directiva 2006/24/CE, 2006; L 105/56).

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

[316] GONZÁLEZ PASCUAL, M.I., *"El Tribunal Constitucional Federal alemán ante…"*, op. cit., p. 947.

[317] Conclusiones del Abogado General Cruz Villalón, de 12 de diciembre de 2013, caso Digital Rights Ireland, C-293/12, apartado 15.

A partir de ese momento, los Estados miembros reformaron sus legislaciones domésticas en la materia, en base a una norma que les habilita a adoptar medidas legales para establecer excepciones a los derechos contenidos en la misma por razones de protección de la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos. El devenir posterior ya lo hemos anunciado[318]:

> "dictaminó que la conservación de datos constituye en sí misma una excepción al deber de garantizar la confidencialidad de las comunicaciones realizadas a través de una red pública de comunicaciones electrónicas disponibles al público que debe ser interpretada de un modo altamente restrictivo, pero una conservación de todos los datos personales de todos los usuarios, durante un periodo de tiempo tan amplio; y en relación con todos los medios de comunicación electrónica, sin diferenciación, limitación o excepción en función del objetivo que se pretende lograr, no era admisible".

Señala con acierto Ortiz-Pradillo (2020; 6)[319] que, tras las sentencias del Tribunal europeo, la adopción de criterios concretos[320] para el establecimiento de un sistema de conservación de datos con carácter preventivo que sea compatible con el Convenio Europeo de Derechos Humanos y la Carta europea se vislumbra muy complicado [aunque no imposible], no tanto para el acceso a los datos [aunque también] como para la conservación, lo que supondrá una tarea difícil para el legislador.

Quizás uno de los *pecados originales* fue la base jurídica escogida sobre la que se apoyó la Directiva, que en este caso ya sabemos que estaba relacionada con la armonización del mercado en la Unión Europea. Fue precisamente esta la razón que llevó a Irlanda a plantear una cuestión prejudicial, al considerar que en realidad se pretendía facilitar la investigación, detección y enjuiciamiento de infracciones penales

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

[319] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones penales..."*, *op. cit.* p. 6.

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

y, en consecuencia, basarse en una *supuesta* armonización del mercado interior no era adecuado y se debía haber usado otra diferente relacionada con los fines reales perseguidos. En este punto de la historia, el Tribunal europeo no avaló la postura irlandesa al determinar que los preceptos de la Directiva se limitaban *"a las actividades de los prestadores de servicios y no regulaba el acceso a los datos ni la explotación por las autoridades policiales o judiciales de los Estados miembros"*[321]. Así, consideró que el almacenamiento de los datos formaba parte de la actividad de los operadores de servicios de telecomunicaciones [en definitiva, el sector privado] y el acceso a esos datos constituía una actividad policial [que es ejercido por el sector público], lo que, según esta autora[322], tenía implicaciones en los derechos fundamentales, ya que el Tribunal europeo no asumió responsabilidades a la hora de decidir sobre los derechos. Sin embargo, sí condicionó las normas nacionales al ser las normas de transposición las que debían establecer las garantías necesarias sobre los derechos afectados. No fue así y, de hecho, tanto determinados tribunales nacionales como el Tribunal de Luxemburgo cuestionaron el alcance de las medidas, su ambigüedad y su falta de proporcionalidad[323]. Como curiosidad, ilustrativa del desenfocado abordaje de la materia en los Estados miembros, sirva lo que revela McIntyre (2008; 328)[324], al referirse a la elaboración de la norma irlandesa: *"Al redactar la legislación, el Departamento de Justicia sólo consultó a la policía. No hubo ningún contacto con las industrias afectadas (porque el Departamento 'sabía que iban a cooperar') ni con el público"*.

Nos parece interesante la reflexión de González Pascual (2014; 950)[325] respecto de que es necesario considerar la información que puede verse comprometida analizada de forma aislada y también en su conjunto; si se produce alguna acción por el ciudadano

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

[322] GONZÁLEZ PASCUAL, M.I., *"El Tribunal Constitucional Federal alemán ante…", op. cit*., p. p. 948.

[323] El Tribunal Constitucional rumano consideró que el almacenamiento suponía una violación de los derechos reconocidos en la Constitución rumana y el CEDH y declaró inconstitucional la ley de transposición; los tribunales checo y alemán también observaron esa misma interferencia en los derechos, aunque no declararon inconstitucional la conservación en sí misma, sino que consideraron que se debía elevar el nivel de las garantías y, para ello, trataron el impacto en la normativa nacional tanto de las medidas como de las salvaguardias. Más adelante veremos que el Tribunal se ha pronunciado muy recientemente respecto de las modificaciones introducidas por la legislación alemana.

[324] McIntyre, T.J., *"Data retention in Ireland: Privacy, policy and proportionality"*, Computer Law and Security Review, Vol. 24, Issue 4, 2008, pp. 326-334, p. 328.

[325] GONZÁLEZ PASCUAL, M.I., *"El Tribunal Constitucional Federal alemán ante…", op. cit*., p. 950.

afectado que justifique la recogida y almacenamiento de los datos; y en qué medida afecta esta información a una actividad concreta de las que compete su tratamiento a las autoridades [en el ámbito de sus competencias estatutarias y legales]. En definitiva: *"no solo es importante el almacenamiento y tratamiento de datos, sino también las acciones públicas subsiguientes"*.

En cuanto al TJUE, en un análisis similar al de los tribunales checo y alemán, en los apartados 39 y 40 de la *Sentencia Digital Rights* dictaminó que no se había producido vulneración del contenido esencial de los derechos previstos en los artículos 7 y 8 de la Carta[326], ya que no se accedía al contenido de las comunicaciones, pero se habían de aplicar las normas de protección de los datos personales. Por lo tanto, no excluía la posibilidad de establecer un régimen de conservación de datos europeo, lo que supuso una ventana de oportunidad muy importante que, eso sí, llevó a la necesidad de buscar y diseñar ese sistema, teniendo en cuenta el resto de la jurisprudencia que también establece esta sentencia y las que vinieron más tarde [todavía hoy no se ha diseñado, ni siquiera se ha establecido el marco general]. Se citan de forma expresa los requisitos generales que ese sistema debe cumplir respecto de la injerencia en los derechos fundamentales, de acuerdo con el artículo 52, apartado 1 de la Carta de derechos fundamentales. La *novedad negativa* la encontramos en que el TJUE considera que en este caso la injerencia es *especialmente grave* y, al respecto, hace consideraciones fundamentales que reflejamos a continuación:

- En este caso, reconoce que la Directiva tiene como objetivo la lucha contra la delincuencia grave y esto justifica, por su especial entidad, la injerencia en los derechos afectados[327].
- Considera a la lucha contra la delincuencia con un objetivo de interés general de la Unión[328]. En este caso, no sorprende el pronunciamiento, ya que otro artículo de la Carta (el artículo 6) reconoce también el derecho a la

[326] Algunos autores consideran que esta decisión del TJUE es polémica, ya que la distinción entre el contenido del mensaje y los metadatos se torna difusa de cara a la protección del derecho a la privacidad, si se tiene en cuenta que la tecnología de vigilancia actual es lo suficientemente invasiva incluso sin acceso al contenido de las comunicaciones. Vid. PUERTO, M.I y SFERRAZZA TAIBI, P., *"La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional"*, en Revista Derecho del Estado, nº 40, enero-junio de 2018, pp. 209-236, p. 227.

[327] Sentencia TJUE, 8 de abril de 2014, caso Digital Rights, apartado 41.

[328] Sentencia TJUE, 8 de abril de 2014, caso Digital Rights, apartado 44.

Seguridad. Como hemos abordado en el primer capítulo, este es un debate de largo recorrido y sujeto a controversia permanente. No obstante, el Tratado de Lisboa, como indica González Pascual, ha reforzado la posición de la UE en este punto[329].

- Centra la atención, como un elemento esencial de análisis y discusión, en el principio de proporcionalidad, reiterando su criterio acerca de la obligación de la normativa europea de no superar los límites de lo que resulta apropiado y necesario para alcanzar los objetivos previstos. En el apartado 50 de la *Sentencia Digital Rights* se incluyen también determinados criterios para establecer el alcance de la facultad de control del Tribunal respecto del cumplimiento o no del principio de proporcionalidad: en función de *"el ámbito afectado, el carácter del derecho en cuestión garantizado por la Carta, la naturaleza y la gravedad de la injerencia, así como la finalidad de esta"*. No es la primera vez que se pronuncia en ese sentido, pues en la Sentencia de 9 de noviembre de 2010, Volker y Markus Schecke GbR Hartmut Eifert, C-92/09 y C-93/09, Rec. P. I-11063[330] ya fijó, en el apartado 86, un estándar superior del principio de proporcionalidad[331]. Respecto de la materia objeto de nuestra investigación, el Tribunal tuvo en cuenta el reforzamiento del principio de proporcionalidad para considerar nula la Directiva europea al considerar, como recoge en los apartados 46 a 58, su

[329] GONZALEZ PASCUAL, M., *"Criminal Law as an Essential Function of the State: Last Line of Resistance?"*, en SAIZ ARNAIZ, A., ALCOBERRO LLIVINA, C. (*eds.) National Constitutional Identity and European Integration, Intersentia, Antwerp,* 2013, pp. 159-175.

[330] Sentencia del TJUE (Gran Sala), de 9 de noviembre de 2010, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, por publicación de información sobre los beneficiarios de ayudas agrícolas. En el apartado 86, el Tribunal establece que: *"Se deduce del conjunto de consideraciones expuestas que no parece que las instituciones hayan ponderado equilibradamente, por un lado, los objetivos del artículo 44 bis del Reglamento 1290/2005 y del Reglamento 259/2008 y, por otro, los derechos que los artículos 7 y 8 de la Carta reconocen a las personas físicas. Dado que las excepciones a la protección de los datos de carácter personal y las limitaciones de dicha protección deben establecerse sin sobrepasar los límites de los estrictamente necesario […] y que cabe concebir medidas que entrañen lesiones de menor gravedad a este derecho fundamental de las personas físicas, sin dejar por ello de contribuir eficazmente al logro de los objetivos de la normativa de la Unión controvertida, procede concluir que el Consejo y la Comisión han sobrepasado los límites que impone el respeto del principio de proporcionalidad al obligar a publicar los nombres de todas las personas físicas beneficiarias de ayudas …"*.

[331] No obstante, no siempre ha sido así. El principio de proporcionalidad se ha aplicado tradicionalmente, según algunos autores, como indica González Pascual, de forma poco exigente, al exigir que una medida sea necesaria y adecuada pero no que sea proporcionada en sentido estricto. Ciertos autores vinculan la precaución del TJUE frente a la proporcionalidad en sentido estricto con el deseo de otorgar un espacio de decisión a los Estados miembros en temas sensibles.

carácter indiscriminado, vago y carente de medidas de protección de la información. [332]

Volviendo al papel del Tribunal de Justicia de la Unión Europea como garante de los derechos y a la cuestión prejudicial como recurso de los ciudadanos en defensa de esos derechos, si bien no siempre es la mejor vía de solución, puede contribuir a la integración o armonización de los sistemas judiciales y, por qué no, descargar también de trabajo a los tribunales nacionales. La determinación de qué casos deberían elevarse al Tribunal europeo y cuáles no queda al criterio nacional, al no existir una guía para los tribunales nacionales sobre qué opción escoger en cada momento. En el *Caso Digital* Rights, puesto que se solicitaba la anulación de una directiva europea, solo existía el recurso a la cuestión prejudicial. Asevera Konstandinides (2011; 736)[333] que se han aprobado normas represivas en la Unión con el pretexto de que son competencia a nivel de los Estados miembros y, de ese modo, se han atribuido competencias a la Unión Europea de forma indirecta y, sin embargo, no se ha considerado al mismo tiempo su impacto en los derechos fundamentales. Sin embargo, los problemas que ciertas normas han generado, como la Directiva 2006/24/CE, solo pueden ser abordados por el Tribunal de Luxemburgo. Es cierto que, como concluye González Pascual (2009; 946)[334], la sentencia *"vino en gran medida condicionada por la cascada de decisiones nacionales contrarias a la norma europea, circunstancia bastante insólita"*.

La pregunta que nos surge a continuación es *¿qué ocurre con las legislaciones nacionales de transposición de la Directiva una vez que el TJUE la declaró inválida?* Analizaremos esta cuestión y sus posibles respuestas más adelante, sobre todo porque a esta primera sentencia han seguido otras igualmente notorias que también debemos abordar antes.

[332]GONZÁLEZ PASCUAL, M.I., *"El Tribunal Constitucional Federal alemán ante…"*, op. cit., p. p. 957.

[333] KONSTANDINIDES, T., *"Destroying the democracy on the Ground of Defending it? The Data Retention Directive, the Surveillance and Our Constitutional Ecosystem"*·, ELRev, 36, 2011, p. 736.

[334] GONZÁLEZ PASCUAL, M.I., *"El Tribunal Constitucional Federal alemán ante…"*, op. cit., p. p. 946.

1. Segunda sentencia. El TJUE confirma su doctrina

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

Al mismo tiempo, en el Reino Unido se puso en duda la legalidad de la Ley de Retención de Datos y Poderes de Investigación de 2014 (DRIPA), que se había promulgado después de la sentencia de *Caso Digital Rights Ireland*. En esta ocasión, el Sr. Watson y otros ciudadanos mostraron preocupación porque la DRIPA podría no ser compatible con la Carta, ni con el Convenio Europeo de Derechos Humanos. En este caso, la nueva ley británica pretendía mantener el sistema de conservación y acceso a los datos que implantó la Directiva 2006/24/CE, con la diferencia de que se presentaba como medida nacional. El Tribunal británico consideró que el TJUE solo cuestionaba la Directiva europea y no las salvaguardas que la norma británica preveía. No obstante, la Corte británica declaró que la DRIPA contravenía los artículos 7 y 8 de la Carta y sostuvo que la Sentencia al *Caso Digital Rights Ireland* era aplicable a las normas de transposición en los Estados miembros. Finalmente, el Tribunal de Apelación planteó una cuestión prejudicial ante el TJUE antes de tomar una decisión respecto de las cuestiones suscitadas en el Reino Unido.

En 2016, en la sentencia del *Caso Tele2 Sverige*[335], el Tribunal resolvió las cuestiones prejudiciales mencionadas y confirmó que la normativa europea, en particular la Directiva de privacidad electrónica, impide que la legislación nacional pueda prescribir una conservación de datos generalizada e indiscriminada. Por el contrario, también dejó claro que esta no impide que la legislación nacional pueda imponer una *"conservación dirigida o específica a los efectos de la lucha contra el*

[335] Casos C-203/15 y C-698/15 Tele 2 Sverige AB and Watson and others, 21 de diciembre de 2016.

delito grave, a condición de que esté limitada a lo estrictamente necesario". Este pronunciamiento mantuvo las esperanzas de quienes estaban analizando la situación desde 2014 para ver cómo cumplir con los requerimientos derivados de la primera sentencia y no *"tirar por tierra"* el trabajo pasado, presente y futuro de los cuerpos policiales y los sumarios judiciales todavía en fase de instrucción en los juzgados y tribunales. Lo cierto es que [adelantándonos a las pinas siguientes] podemos decir el moderado optimismo generado por este importante matiz que introducía la sentencia de 2016 no duró demasiado. Hasta ese momento, pero también a raíz de la nueva intervención del Alto Tribunal, la doctrina no se había mostrado unida acerca de si las leyes nacionales derivadas de la Directiva invalidada también perdían su vigencia. A la vista de esta sentencia, nos podría parecer indubitado que así es. Sin embargo, como recoge Polo Roca (2021; 7)[336], aunque unos autores consideraban que la regulación de la conservación de datos recaería a partir de ese momento de nuevo sobre la facultad otorgada por el artículo 15, apartado 1 de la norma europea sobre privacidad de las comunicaciones, otros, citando a Encinar del Pozo (2014)[337], defendían la pérdida de su vigencia.

El TJUE fijó también en esta ocasión las salvaguardas que han de ser respetadas a la hora de establecer normativas nacionales, a saber:

- La conservación de los datos sin contenido debe ser la excepción;
- El propósito de la conservación debe ser restringido a la lucha contra el delito grave;
- Debe ser limitada a lo estrictamente necesario;
- El acceso a la información conservada debe ser objeto de revisión previa por un tribunal o autoridad independiente;
- La información debe ser conservada solo dentro de la Unión Europea.

[336] POLO ROCA, A., La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión, IDP núm. 33, 2021, pp. 1-16, p. 7.

[337] Cfr. ENCINAR DEL POZO, M.A., *"La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones"*, Topo Jurídico Nuevas Tecnologías, SEPIN, 2014.

Esta sentencia de 21 de diciembre de 2016[338] se diferencia fundamentalmente de la decisión anterior en el *Caso Digital Rights Ireland* por el hecho de que lo que se cuestiona no es una directiva de la Unión Europea, sino la legislación nacional de alguno de sus Estados miembros[339]. Creemos también sobresaliente que esta sentencia resuelve una duda generalizada en los Estados miembros y que tendrá repercusiones directas, irremediables y notorias sobre las legislaciones del resto de miembros [aún no lo ha tenido en los veintisiete; sí en algunos de ellos][340].

El TJUE se centra en la cuestión de si el artículo 15, apartado 1 de la Directiva sobre privacidad y las comunicaciones electrónicas, teniendo en cuenta los artículos 7, 8 y 52, apartado 1 de la Carta *"... debe interpretarse en el sentido de que se opone a una legislación nacional... para la conservación general e indiscriminada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados con respecto a todos los medios de comunicación electrónica"*. La sentencia enmarca los espacios de las excepciones del artículo 15, apartado 1, al exigir que estas se consideren de manera excepcional, de forma que los Estados no puedan esgrimir, según indica en el apartado 91, razones especiales relacionadas con la seguridad pública para restringir de una forma razonable la protección de los derechos fundamentales recogidos en la Carta y, en consecuencia, la normativa nacional debe prever que la excepción al principio de confidencialidad debe guardar relación con la gravedad de la intromisión en los derechos fundamentales que representa el acceso, por lo que la justificación estará en la lucha contra el terrorismo y la delincuencia grave[341].

Las comunicaciones electrónicas, incluidos los datos de tráfico, deben ser, como principio general, confidenciales, tal y como se indica en el apartado 1 del artículo 5 de la Directiva de 2002: *".... Como norma general, se prohíbe que cualquier persona distinta de los usuarios almacene, sin el consentimiento de los usuarios afectados, los datos de tráfico relacionados con las comunicaciones electrónicas"*. Sin embargo, el

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

[339] En aquel momento, Reino Unido formaba parte aún de la Unión Europea.

[340] Nombre con el que de forma coloquial y extendida se denomina a los Estados miembros de la Unión Europea, que han pasado a ser 27 desde la salida del Reino Unido de la Unión.

[341] Sentencia TJUE, de 21 de diciembre de 2016, caso *Tele2 Sverige*, apartado 115.

apartado 1 del tan repetido artículo 15 constituye una importante excepción al principio de confidencialidad, ya que permite la retención o interceptación de determinados datos [no pocos].

El Tribunal considera también que la excepción prevista en el apartado 1 del artículo 15 "*debe interpretarse estrictamente"*. Además, establece que la norma general prevista en el artículo 5 no puede ser sustituida ni anulada por la excepción. La normativa nacional debe respetar los principios del Derecho de la Unión, incluida la Carta. Recordando el apartado 1 del artículo 52 de , las limitaciones a los derechos garantizados *"…. deben estar previstos por la ley y respetar la esencia de dichos derechos y libertades"*. Como hemos analizado en apartados anteriores, las restricciones a la protección de datos personales en combinación con el derecho al respeto de la vida privada sólo se permiten si son estrictamente necesarias, al menos en el ámbito de la Unión Europea y de acuerdo con la jurisprudencia del TJUE.

Por lo anterior, podemos concluir que el Tribunal confirmó su jurisprudencia, declarando que la conservación general de los datos personales no puede convertirse en una norma y, para cumplir con la Carta, la retención tiene que limitarse a lo estrictamente necesario, debiendo existir siempre un vínculo entre los datos conservados y la finalidad perseguida, lo que exige evaluar qué tipo de datos pueden ser potencialmente relevantes para su conservación a efectos de la prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales, incluida la salvaguardia y la prevención de amenazas a la seguridad pública. Además, el Tribunal exige también en la sentencia que el acceso a los datos retenidos sea específico e incluya garantías adicionales, como un periodo de almacenamiento limitado, normas de acceso diferenciadas, una supervisión adecuada, etcétera.

Cita Rizzo (2019; 399)[342] una frase incluida por el Abogado General de la Unión Europea que ilustra la continuidad del Tribunal en su tesis adoptada en la Sentencia del *Caso Digital Rights Ireland*: *"si los hombres fueran como ángeles, no sería necesario*

[342] RIZZO, G., *Derecho a la privacidad...*, op. cit., p.399.

gobierno alguno. Si los ángeles gobernaran a los hombres, no sería necesario ningún control externo o interno sobe el gobierno. Al organizar un gobierno de hombres para hombres, la gran dificultad estriba en esto: primero hay que capacitar al gobierno para que controle a los gobernados; luego hay que obligarle a que se controle a sí mismo"[343]. En realidad, aquí se dilucida la capacidad de los parlamentos nacionales para adoptar normas de conservación de datos en transposición de una norma europea que les permita actuar de forma eficiente en la lucha contra el terrorismo y la delincuencia grave que amenazan a la seguridad de sus conciudadanos y, al mismo tiempo, que estas sean respetuosas con los derechos fundamentales que les asisten. Una vez más, el pensamiento nos lleva rápidamente al dilema *Libertad vs. Seguridad*.

Con cierto desacuerdo en este importante aspecto, considera Ortiz-Pradillo (2020; 10)[344] que, según rezan los apartados 104 y siguientes de las Conclusiones a los Asuntos C-511 y 512/18 y apartados 105 y siguientes de las Conclusiones al Asunto C-520/18:

> *"en situaciones propiamente excepcionales, caracterizadas por una amenaza inminente o por un riesgo extraordinario que justifiquen la declaración oficial de la situación de emergencia en un Estado miembro, la legislación nacional complete, por un tiempo limitado, la posibilidad de imponer una obligación de conservación de datos tan amplia y general como se considere imprescindible."*,

pero esta situación puede abrir la puerta a que estos argumentos y justificaciones sean reconducidos hacia *amenazas graves y persistentes a la seguridad nacional* o provocadas por causas achacables al terrorismo, y permita a los Estados miembros dar respuestas diferentes.

La legislación sueca preveía un régimen de retención de datos *general e indiscriminado* que almacenaba todos los datos de tráfico sin ninguna excepción. Se

[343] Conclusiones del Abogado General Sr. Henrik Saugmandsgaard Oc. De 19 de julio de 2016, en los Asuntos acumulados C-203/15 y C-698/15, Tele 2 Sverige AB contra Post- och telestyrelsen (C-203/15) y Secretary of State for the Home Department contra Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15), en http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=ES

[344] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones penales…"*, op. cit., p. 10

trataba, en efecto, de un régimen muy similar al creado por la invalidada Directiva de 2006.

Al igual que en el Caso *Digital Rights Ireland*, el Tribunal de Luxemburgo afirma en este caso que la interferencia en los derechos es de *"gran alcance"* y *"especialmente grave"* y que la población afectada podría sentir una *"vigilancia constante"* y concluye que *"una normativa nacional como la controvertida en el litigio principal rebasa, por tanto, los límites de lo estrictamente necesario y no puede considerarse justificada, en el marco de una sociedad democrática, como exige el artículo 15, apartado 1 de la Directiva 2002/58/CE, leído a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta"*.

Aun habiendo confirmado su doctrina, no rechaza la idea de la conservación de datos por un Estado miembro que pueda aprobar una legislación con *"... la conservación selectiva de datos de tráfico y de localización, con el objetivo de luchar contra la delincuencia grave, siempre que la conservación de los datos se limite a lo estrictamente necesario, en lo que respecta a las categorías de datos que deben conservarse, los medios de comunicación afectados, las personas afectadas y el período de conservación adoptado"*.

A continuación, el TJUE examina un segundo punto: si es compatible con la Carta de los Derechos Fundamentales de la Unión Europea *"... el acceso de las autoridades nacionales competentes a los datos conservados, cuando dicha legislación no restringe el acceso únicamente al objetivo de luchar contra la delincuencia grave, cuando dicho acceso no está sujeto a un control previo por parte de un tribunal o de una autoridad administrativa independiente, y cuando no se exige que los datos en cuestión se conserven en la Unión Europea"*.

El acceso a los datos conservados sólo puede realizarse si está *"verdadera y estrictamente"* relacionado con uno de los elementos enumerados en el apartado 1 del artículo 15 y este acceso sólo es posible, en lo que respecta al ámbito de la persecución

de delitos, para el *"objetivo de luchar contra la delincuencia grave"* debido a su colisión con los derechos fundamentales. De ello se desprende que el acceso no es admisible para la lucha contra los delitos que no son graves y este se reducirá a lo *"estrictamente necesario"*. Asimismo, debe ser concedido por autoridades judiciales o administrativas independientes y los datos deben conservarse en la Unión Europea, con el fin de proteger la aplicabilidad de la jurisdicción. Aclara también que en *"situaciones particulares"*, como las que tienen que ver con la seguridad nacional, la defensa o la seguridad pública, podría concederse el acceso a los datos cuando *"existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra dichas actividades"*[345].

El Tribunal sentencia que la Carta excluye *"... el acceso de las autoridades nacionales competentes a los datos retenidos, cuando el objetivo perseguido por dicho acceso, en el contexto de la lucha contra la delincuencia, no se limite únicamente a la lucha contra la delincuencia grave, cuando el acceso no esté sujeto al control previo de un tribunal o de una autoridad administrativa independiente y cuando no se exija que los datos en cuestión se conserven en la Unión Europea"*. Respecto el principio de proporcionalidad, en los apartados 105 y 107, admite otra vez -como ya hizo en el *Caso Digital Rights Ireland*- que solo se puede considerar que no infringen la legislación de la Unión las normas de los Estados miembros que proporcionan *"una conservación de datos referentes a un periodo temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia"*[346].

Esto hace que el juez o la autoridad administrativa que autorizan el acceso a los datos, en su resolución motivada deben realizar un juicio de proporcionalidad entre la gravedad de la injerencia en los derechos fundamentales y la gravedad de los hechos delictivos, de forma que solo en los casos de delitos graves se debería admitir el acceso a datos electrónicos de carácter personal que supongan una intromisión grave en los

[345] Sentencia TJUE, de 21 de diciembre de 2016, caso *Tele2 Sverige*, apartado 119.
[346] Sentencia TJUE, de 21 de diciembre de 2016, caso *Tele2 Sverige*, apartado106.

derechos a la privacidad y a la protección de los datos personales. En ese juicio de proporcionalidad, deberán ponderar la gravedad de la injerencia y la gravedad del delito. En ese sentido, en la Sentencia del *Caso Tele2 Sverige y Watson* el Tribunal confirma su jurisprudencia anterior y, en consecuencia, confirma también que acceder a las comunicaciones efectuadas con un teléfono [sin contenido] para, entre otros motivos, conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas; así como para obtener los lugares en que estas tuvieron lugar o la localización del terminal; o saber la frecuencia con que estas se realizan en un determinado periodo de tiempo, son injerencias especialmente graves. Por tanto, una injerencia así solo estará justificada para los supuestos que ya hemos analizado y, respecto de los delitos investigados, solo para aquellos que sean considerados como graves. La conclusión más relevante que podemos extraer de lo anterior, en términos de consecuencias más o menos inmediatas, es el fin de las legislaciones nacionales de transposición de la Directiva invalidada. Aun así, tampoco hay un criterio uniforme entre los expertos, ni entre los Estados miembros y, como señala Ortiz-Pradillo (2020; 7), al referirse a la ley española 25/2007, de transposición de la Directiva 2006/24/CE:

> *"resulta muy loable la defensa numantina que tanto el Tribunal Supremo como ciertos autores hacen del sistema española de conservación de datos de comunicaciones electrónicas, pero el mismo no puede seguir considerándose un reino de taifas inmune a los parámetros y garantías exigidas por el Tribunal de Luxemburgo"*[347].

Lo cierto es que hasta la fecha no tenemos constancia de que la ley española se haya dejado de aplicar por jueces y tribunales, ni de que se haya presentado cuestión prejudicial alguna ante la Corte de Luxemburgo. Coincidimos con Ortiz-Pradillo en su pronóstico acerca de que, llegado el caso [y es cuestión de tiempo que esto ocurra], los jueces y tribunales españoles considerarán que la ley resulta incompatible con el derecho europeo y dejen de aplicarla. Las consecuencias de esta situación podrían ser nefastas para procedimientos todavía en fase de instrucción sobre delitos graves en los que los autores podrían quedar sin castigo por sus acciones y, por otro lado, debilitaría la responsabilidad que el Estado tiene sobre sus ciudadanos a la hora de garantizar el

[347] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones penales…", op. cit.*, p. 7

disfrute de otros derechos igualmente importantes y el ejercicio de las libertades públicas.

Con este nuevo pronunciamiento, el Alto Tribunal también aporta otro elemento novedoso e importante: el vínculo entre las disposiciones del Derecho primario de la Unión y los actos derivados -en este caso, las normas de transposición de una directiva. Consideran Fernández-Lasquetty y Bello (2017; 140) que tras esta sentencia la Directiva 2002/58/CE de privacidad electrónica debe interpretarse también [a la luz de la Carta] en el sentido de que se opone a una normativa nacional que interfiera de forma similar a como lo hacía la Directiva 2006/24/CE de forma masiva en el derecho a la protección de los datos personales de los ciudadanos europeos[348]. Los acontecimientos posteriores, cinco años después, les han dado la razón, y lo analizaremos en las pinas finales de este capítulo.

Respecto del concepto de gravedad del delito, nos surge la siguiente pregunta: *¿cómo podemos establecer o hemos de considerar que un delito es grave?* Antes de buscar respuesta a esta pregunta, analizaremos otra sentencia del Tribunal de Luxemburgo, que aporta elementos interesantes precisamente respecto de esta cuestión; sentencia que se ha venido en llamar como el *Caso Ministerio Fiscal*, dictada a resultas de una cuestión prejudicial planteada por un tribunal español: la Audiencia provincial de Tarragona.

2. Caso C-207/16 Ministerio Fiscal

La condición relativa a la gravedad del delito fue posteriormente especificada en el *Caso C-207/16 Ministerio Fiscal*[349], en el que el Tribunal estableció que *"si el acceso a determinados tipos de metadatos no representa una interferencia grave en los derechos fundamentales de privacidad y protección de los datos personales, las*

[348] FERNANDEZ-LASQUETTY, J. y BELLO, M., (2017), *"La legislación europea no permite una normativa nacional que recopile datos de tráfico y localización de manera indiscriminada. Sentencia del Tribunal de Justicia de 21 de diciembre de 2016, Tele2 Sverige (C-203/15 y C-698/15)"*, en *Anuario ELZABURU de jurisprudencia europea en propiedad industrial e intelectual*, pp. 139-141, en http://www.elzaburu.es/en/document-centre/search-news-items?op=viewcms&id2=3005116

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

agencias encargadas de la aplicación de la ley podrán acceder a ellos para la investigación y persecución de delitos no graves".

Un informe de 2017 de *Privacy International*[350] indica que, en muchos Estados miembros, los regímenes de conservación de datos están basados en la Directiva anulada y, en consecuencia, no cumplen con la jurisprudencia del Tribunal europeo. Este informe estima además que los regímenes nacionales de conservación de datos están frecuentemente desactualizados y adolecen de claridad legal, y algunos de ellos se encuentran sometidos a procedimientos de legalidad ante los tribunales nacionales, generando todo ello incertidumbre legal.

Otras citas destacadas de la sentencia relacionadas de forma específica con la protección de los datos personales y con implicaciones en la privacidad son las siguientes [alguna de ellas ya mencionada anteriormente, pero creemos que debe ser recordada y puesta en relación con otras para obtener una perspectiva de conjunto]:

- *el hecho de que la información sea retenida y usada sin que el suscriptor o abonado sea informado puede generar en las personas afectadas el sentimiento de que su privacidad está siendo sujeta a constante vigilancia*[351]*;*
- *se aplica a personas sobre las que no hay evidencia de que sus conductas puedan tener relación, ni directa ni indirectamente, con delitos graves. Además, no se prevé ninguna excepción aplicable a personas cuyas comunicaciones, de acuerdo con la normativa nacional, estén sometidas a secreto profesional*[352]*;*
- *además, a la vez de contribuir a la lucha contra el delito grave, la Directiva 2006/24/CE no requiere ninguna relación entre los datos cuya conservación está prevista y un riesgo para la seguridad pública y, en particular, no está restringida a una retención en relación i) a datos relativos a un momento determinado y/o a un área geográfica concreta y/o ii) a un círculo particular*

[350] Privacy International (2017). National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, September 2017.
[351] Sentencia TJUE, de 8 de abril de 2014, *caso Digital Rights Ireland*, párrafo 37.
[352] Sentencia TJUE, de 8 de abril de 2014, *caso Digital Rights Ireland*, párrafo 58.

de personas que puedan, por otras razones, contribuir, mediante la retención de sus datos, a prevenir, detectar o perseguir los delitos graves[353]*;*

- *... la Directiva 2006/24/CE no prevé ningún criterio objetivo mediante el que el número de personas autorizadas a acceder y, consecuentemente, a usar los datos conservados esté limitado a lo estrictamente necesario en función del objetivo perseguido*[354].

La Sentencia *en el Caso Ministerio Fiscal* es una decisión del TJUE del 2 de octubre de 2018, en el *Caso C-207*, que se refiere principalmente al acceso a los datos retenidos y no a la conservación de los datos en sí. En cualquier caso, consideramos que sus conclusiones también son importantes para la futura jurisprudencia sobre conservación de datos, así como para los legisladores y los tribunales de los Estados miembros, por lo que procede incluirla también en este estudio.

La Audiencia provincial de Tarragona presentó una cuestión prejudicial sobre la base de los siguientes hechos:

> *"Un teléfono había sido robado y la policía, para aclarar las circunstancias, presentó una solicitud para obtener acceso a los datos conservados sobre el teléfono. El alcance de la solicitud era limitado: los datos de los abonados (nombre, apellidos, domicilio y número de teléfono) de las tarjetas SIM que se habían activado en el número de teléfono robado en los primeros doce días después del robo. La solicitud se dirigió al juez competente que debía autorizar el acceso. En primera instancia, sin embargo, lo denegó porque el delito que se estaba investigando no está calificado como delito grave".* En segunda instancia, la cuestión se remitió a Luxemburgo.

La primera consideración a tener en cuenta antes de conocer el fallo del Alto Tribunal es que, a la luz de la sentencia del *Caso Tele2 Sverige*, la cuestión planteada por la Audiencia Provincial de Tarragona [puesto que se preguntaba explícitamente por

[353] Sentencia TJUE, de 8 de abril de 2014, *caso Digital Rights Ireland*, párrafo 59.
[354] Sentencia TJUE, de 8 de abril de 2014, *caso Digital Rights Ireland*, párrafo 62.

el modo de proceder de acuerdo con la legislación española en la materia, y la legislación española sobre conservación de datos procede básicamente de la norma europea invalidada] podría haber dado lugar a que el régimen español de conservación de datos fuera declarado contrario al Derecho de la Unión Europea, como ocurrió tras la decisión de un tribunal sueco. Sin embargo, el Alto Tribunal interpretó el alcance de la cuestión de forma diferente y redujo la cuestión a aspectos de acceso a los datos, pasando por alto la conservación. Esto significa, esencialmente, que el Tribunal no juzgó el régimen español de conservación de datos, sino sólo el procedimiento de acceso a la información conservada. Por lo tanto, lo que en realidad se estaba discutiendo eran las condiciones y circunstancias para disponer de los datos que habían sido retenidos por el proveedor de servicios de telecomunicaciones.

En *Tele2 Sverige*, el Tribunal declaró que el acceso a los datos por parte de las autoridades sólo es legal en los casos de investigación de los *"delitos graves"*. En el *Caso Ministerio Fiscal*, sin embargo, estima que esta consideración es demasiado estricta y modifica su interpretación. Esto supone un cambio de criterio de gran importancia y así ha sido tomado por los decisores políticos, a través de los técnicos que discuten cómo afrontar la situación derivada de la anulación de la norma europea de 2006.

Según esta sentencia, el acceso a los datos retenidos puede concederse incluso en los casos en los que no se investigan *"delitos graves"*, siempre que se tenga en consideración la proporcionalidad de la medida. Una vez más, surge la exigencia de realizar una prueba de proporcionalidad, que será determinante a los efectos de valorar si el acceso realizado cumple o no con la doctrina sentada por la Corte de Luxemburgo. En ese sentido, el Tribunal decide que:

> *"el acceso a los datos de los abonados de las tarjetas SIM activadas en el teléfono en los primeros doce días tras el robo es proporcional; estos datos no revelan información sustancial y precisa del afectado y no constituyen, por tanto, una injerencia grave en los derechos fundamentales que permita obtener conclusiones precisas sobre la vida privada del afectado"*.

Podríamos sostener, sin exagerar, que la sentencia no es tan *garantista o exigente* como la del *Caso Tele2 Sverige,* e incluso que fija el límite de acceso a los datos por debajo de la Directiva invalidada, encontrando posible que sea efectuado también para delitos no graves, siempre que la acción concreta no constituya una injerencia grave en los derechos fundamentales. Es decir, ahora, el criterio de gravedad del delito queda matizado o ponderado mediante la valoración de la medida de acceso a los datos en función de su mayor o menor interferencia en los derechos fundamentales en juego.

El Abogado General Campos Sánchez-Bordona, en sus Conclusiones al *Caso C-520/18*[355] defiende que no se han producido cambios en el parecer del Tribunal y que no se autoriza en ningún caso un régimen nacional de conservación masiva e indiscriminada de datos personales, de modo que no hay modificación respecto de la doctrina expresada en la *Sentencia del Caso Tele2 Sverige y Watson*. Por su parte, sin oponerse al criterio del Abogado General, Ortiz-Pradillo (2020; 7)[356] lamenta que el TJUE no contestó a dos cuestiones fundamentales que habían sido incluidas en la cuestión prejudicial respecto de la que se pronunció y, por esa ausencia de respuesta, cree que no entró [o no quiso entrar] en el fondo de las dudas que se le habían trasladado:

"i) si la gravedad del delito que justifica la injerencia en los derechos fundamentales puede identificarse únicamente por la pena que puede imponerse al delito que se investiga o también se deben identificar en la conducta niveles particulares de lesividad para bienes jurídicos individuales y/o colectivos, y

ii) si un umbral mínimo de 3 años se ajusta a los principios constitucionales de la Unión[357].

Para Peralta Gutiérrez y Aguirre Allende (2019; 9)[358], lo que se dilucidaba era la relación entre la normativa europea [la Directiva de conservación de datos] y la

[355] Apartados 66 y 67 de las Conclusiones del Abogado General de la UE, Campos Sánchez-Bordona.

[356] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones penales…", op. cit.,* p. 7

[357] *Ibíd*. p. 8.

competencia de los Estados miembros en cuanto a sus capacidades de investigación penal garantizados por los Tratados de la Unión y el resto de los instrumentos de derecho originario. El propio Abogado General, como indican los autores antes reseñados, hizo suya la postura del Ministerio Fiscal español respecto al propósito de los cuerpos policiales afectados, que no era otro que: *"recoger información que no se refiere ni a una localización ni a comunicaciones como tales, sino a personas físicas buscadas por haber podido utilizar un servicio de comunicaciones electrónicas mediante el teléfono sustraído, aunque no hayan realizado llamada telefónica concreta"*[359]. Sigue el Abogado General con su argumentación en los apartados 78 y 86 de las Conclusiones y llama a esa información como *"datos de contacto"* que, a pesar de que su acceso constituye una injerencia en los derechos fundamentales, a diferencia de los supuestos contemplados en las sentencias de 2014 y 2016, *"no reviste un carácter particularmente grave"*. Esa diferencia hace que la respuesta para este tipo de situaciones debería ser diferente también a la que el Tribunal adoptó en las anteriores sentencias. Y así lo hizo el Tribunal de Luxemburgo al considerar en el apartado 63 de la Sentencia en el *Caso Ministerio Fiscal* que *"un acceso tal no presenta una gravedad tal que […] deba limitarse […] a la lucha contra la delincuencia grave"*.

Las Conclusiones del Abogado General también se refieren a esta cuestión al considerar que no se debe tener en cuenta únicamente la sanción aplicable a la hora de determinar la gravedad del delito (apartado 93). Por tanto, será preciso valorar también otros criterios, que Ortiz-Pradillo (2020; 7)[360] enumera (entre otros):

> *"la naturaleza de las infracciones, el daño que causan a la sociedad, el menoscabo que provocan en los intereses jurídicos y los efectos generales que producen en el ordenamiento jurídico nacional, así como en los valores de una sociedad democrática, el contexto histórico, económico y social específico de*

[358] PERALTA GUTIÉRREZ, A., y AGUIRRE ALLENDE, P., *"El TJUE y el acceso a los datos de abonado en el seno de la instrucción penal"*, en Diario La Ley, nº. 9420, Sección Tribuna, 22 de mayo de 2019, pp. 1-17, p.9 Wolters Klumer, en https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params

[359] Apartado 36 de las Conclusiones del Abogado General.

[360] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones penales…"*, *op. cit.*, p. 7.

cada Estado miembro o si los delitos han sido cometidos, bien de manera reiterada, bien contra colectivos vulnerables".

Estos criterios u otros que se puedan considerar permitirían a la autoridad habilitada para autorizar la medida a ponderar la proporcionalidad de la injerencia en los derechos afectados y, junto con la sanción aplicable, se gradaría el mayor o menor acceso a los datos conservados. En definitiva, se permitiría establecer un acceso limitado, como prescribe el Tribunal de Luxemburgo.

3. Situación en los Estados miembros tras las primeras sentencias

Según establece el artículo 266 del TFUE *"la institución, órgano u organismo del que emane el acto anulado, o cuya abstención haya sido declarada contraria a los Tratados, estará obligado a adoptar las medidas necesarias para la ejecución de la sentencia del Tribunal de Justicia de la Unión Europea"*.

Se plantea a continuación la cuestión respecto de los efectos prácticos sobre los tribunales nacionales de una declaración de nulidad de una norma europea, sobre las consecuencias ante una legislación incompatible con el Derecho de la Unión Europea o acerca de cómo serían las leyes nacionales de transposición de una Directiva inválida, como la 2006/24/CE, entre otras.

Este es también un debate controvertido, nada pacífico. A efectos prácticos, la declaración de invalidez de la Directiva no ha anulado de forma automática las normativas nacionales de transposición por el simple hecho de que esta ya no sea aplicable, incluso aunque, como ya indicamos, fue declarada inválida "*ex tunc"*. Al contrario, los tribunales nacionales, a la hora de dictar sentencia deben continuar aplicando las normativas nacionales y valorar caso por caso (y así lo hacen) su validez. Si la mantienen, deberán valorar la información y las pruebas que se hubieran obtenido en base a facultades que han sido anuladas por el Tribunal europeo y que, en ese momento, son ya contrarias al Derecho de la Unión; en definitiva, deberán tomar en consideración si se ven respetados o no los derechos fundamentales respectivos en cada uno de los casos que se encuentran enjuiciando. A diferencia de lo que se podía pensar,

algunos Estados miembros vieron en la anulación de la Directiva una oportunidad para actuar con sus normativas nacionales sin el corsé que suponía la norma europea, de forma que, si bien no se conseguía la armonización pretendida a nivel de los Estados miembros, tampoco se establecían restricciones a los sistemas nacionales y se volvía a la situación anterior en la que las concesiones propias de una negociación como esta, suponían asumir determinados postulados que no beneficiaban a todos los países. En consecuencia, con la nulidad de la Directiva, ya no tendrían efecto. No obstante, ya en aquel momento [hoy ya no cabe duda, puesto que el TJUE lo ha dejado meridianamente claro en sentencias posteriores que analizaremos a continuación] eran muchas las voces autorizadas que indicaban que, anulada la Directiva 2006/24/EC, se volvía a los preceptos del artículo 15, apartado 1 de la Directiva de privacidad electrónica.

En este sentido, relata lo siguiente el Abogado General de la UE en sus Conclusiones al *Caso C-746/18*[361] (2021; apartados 47 y 48):

> *"si bien es cierto que el Derecho de la Unión no se aplica, en el estado actual de su evolución, a las normas que regulan la admisibilidad de las pruebas en el proceso penal, […] la admisibilidad de las pruebas depende de que se respeten los requisitos y normas procesales que regulan la obtención de esas pruebas […]. Así pues, en este aspecto, las normas nacionales aplicables en materia de práctica de la prueba deben respetar las exigencias derivadas de los derechos fundamentales garantizados por el Derecho de la Unión"* (Conclusiones del Abogado General UE, 2021; apartados 47 y 48). Por consiguiente, no podrían ser tenidas en cuenta las pruebas obtenidas a través de un sistema que no sea respetuoso con los artículos 7, 8, 11 y 52 de la Carta.

Por otro lado, dentro de la controversia apuntada al comienzo, hay otros autores que no albergan duda alguna respecto de la pérdida de vigencia de las normativas nacionales, a la luz de la Sentencia del *Caso Tele2 Sverige* y según lo recogido en el artículo 288 del TFUE, según el cual las directivas conllevan una *"obligación de resultado"* y son los Estados miembros quienes eligen la forma y los medios para

[361] Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, caso C-746/18, apartados 47 y 48.

cumplir esa obligación. De no ser así, sostiene Polo Roca (2021; 8)[362], daría lugar a una incorrecta transposición de la norma con supuestos tales como: *"la divergencia regulatoria, la doble regulación, el deslizamiento regulatorio o la sobrerregulación"*[363]. Dejaremos al margen de este trabajo la polémica y mantendremos que una directiva establece unas normas mínimas que deben incorporar las normativas nacionales de transposición, pero que una y las otras son normas diferentes e independientes, aunque el contenido de la Directiva europea, como mínimo, deba ser recogido por la normativa nacional.

El debate público sobre las implicaciones en la privacidad de la Directiva 2006/24/CE, que como decíamos comenzó incluso antes de que esta se aprobara con la redacción de ese año, se vio claramente reforzado por la sentencia de 2014. Ciudadanos y grupos de interés en muchos Estados miembros cuestionaron entonces las normativas nacionales en la materia bajo el argumento de la doctrina del *fruto del árbol envenenado* que, aunque no es propiamente aplicable a nuestro caso, indica que la invalidación de la Directiva produciría el efecto indefectible de contaminar también a las normas nacionales que de ella derivaron y con efectos desde el mismo día de su entrada en vigor.

Europol realizó en 2017 una encuesta entre los Estados miembros[364] que reveló que en siete de ellos (Austria, Bulgaria, Alemania, Países Bajos, Polonia, Eslovenia y Eslovaquia) la normativa en materia de conservación de datos había dejado de estar vigente y, entre los que sí mantenían su vigencia (al menos en tres: España, Finlandia y Hungría), se había revisado o se encontraba en proceso de revisión.

Al mismo tiempo, los países participantes en la encuesta confirmaron *de forma anónima* que la conservación de datos había producido un impacto positivo en la

[362] POLO ROCA, A., *"La regulación sobre la conservación de datos…"* op. cit, p. 8.

[363] RENDA, A. (2009), *"Policy-making in the EU: achievements, challenges and proposals for reform"*. Brussels: Centre for European Policy Studies (CEPS), pp. 1-90, pp. 76 y 77.

[364] Europol, Data Protection Office. EDOC#791813 (Study on the Data Retention Regime Applied in the EU Member States).

prevención, investigación y persecución de los delitos graves y el terrorismo, como reconoce también la propia Sentencia en el *Caso Digital Rights Ireland*[365].

Este tipo de datos no suelen ser prueba determinante, pero facilitan la investigación. De forma particular, en casos de explotación sexual de menores y *grooming*[366], homicidios[367], terrorismo[368] y ciberataques, los participantes en la encuesta enfatizaron la importancia de la conservación de datos para poder discernir o corroborar otras pruebas, y vincular a sospechosos y víctimas o localizar a personas desaparecidas. En ausencia de otras pruebas forenses o testimonios de testigos, la información retenida es en muchas ocasiones la única herramienta disponible para iniciar una investigación. De forma adicional, esta información permite establecer elementos de prueba que conduzcan al esclarecimiento de un delito y que apoyen la decisión judicial en la toma de decisiones.

Reiteramos que estas sentencias constituyen un cambio importante en el papel que el Tribunal de Luxemburgo asume en la defensa de los derechos fundamentales de los europeos, independizándose en gran medida del Tribunal de Derechos Humanos de Estrasburgo. Sin embargo, al no desplegar efectos inmediatos sobre las normativas nacionales de los Estados miembros, su eficacia no puede considerarse garantizada o acreditada a priori. Antes de valorar la reacción de algunos Estados miembros a los fallos del Tribunal, nos detendremos en determinadas cuestiones particulares derivadas de estas, por las directas implicaciones en el trabajo de las autoridades policiales y judiciales.

---

[365] Sentencia TJUE, de 8 de abril de 2014, *caso Digital Rights Ireland*, párrafo 49.

[366] Vid. Caso de grooming in Rochdale (UK), que llevó a diversas condenas en el contexto de la "Operación Doublet", relativas a abusos sexuales que se produjeron entre 2005 y 2013, en https://www.theguardian.com/uk-news/2016/apr/08/rochdale-grooming-case-10-men-sentenced-to-up-to-25-years-in-jail, visitada el 10 de julio de 2021,

[367] Vid. Caso *"Soham Murders",* relativo al homicidio de Holly Marie Wells y Jessica Aimee Chapman, ambas de 10 años, asesinadas en agosto de 2002 en Cambridgeshire, en https://www.manchestereveningnews.co.uk/news/uk-news/soham-murders-what-happened-holly-24671330, visitado el 10 de julio de 2021.

[368] Vid. Ataques terroristas al aeropuerto de Glasgow en 2007, https://www.elconfidencial.com/mundo/2007-07-02/otros-dos-detenidos-en-relacion-con-los-ataques-contra-el-aeropuerto-de-glasgow_371621 visitado el 10 de julio de 2021.

3.1 Falta de una definición clara sobre qué es un delito grave

La falta de una definición concreta y específica de lo que puede considerarse como delito grave genera un panorama fragmentado entre los Estados miembros, como confirmó la encuesta antes mencionada que elaboró Europol. Estamos de acuerdo con Arroyo Romero (2006; 89)[369] cuando estudia la necesidad de otorgar a Europol más atribuciones en materia de investigación [es cierto que desde 2005 esta agencia ha avanzado notablemente en cuando a competencias y medios para ejercerlas] y concluye que ello requeriría de reformas legislativas que deberían llevar a los Estados miembros a asumir que el *ius punendi* no quedaría limitado porque sus ordenamientos jurídicos compartieran iguales regulaciones de determinados tipos penales. Cita el autor también la intervención del Director del Servicio Nacional de Inteligencia Criminal del Reino Unido, de septiembre de 2002, en la que recordaba que la lentitud en el intercambio de información y la falta de una definición común de delitos, beneficia a la delincuencia organizada.

En la mayoría de los países, la determinación de la gravedad se basaba en una evaluación cuantitativa del período mínimo de privación de libertad: 5 años en cinco de ellos (Bulgaria, Chipre, España, Portugal y Eslovaquia), y 4 años en otros seis (Austria, República Checa, Lituania, Países Bajos, Polonia y Reino Unido). Además, el estudio reveló que, en al menos tres países (República Checa, Países Bajos y Portugal), la normativa establecía de forma adicional la realización de un análisis cualitativo sobre la gravedad del delito[370].

Respecto de cuándo un delito tiene la consideración de grave, el Tribunal europeo no se pronuncia de forma expresa en ninguna de las tres sentencias principales que hemos tratado, incluso habiéndose cuestionado de forma expresa en el *Caso Ministerio Fiscal*. La Sentencia Tele2 Sverige y Watson se limita a relacionarla con la delincuencia organizada y el terrorismo. No obstante, no solo en el ámbito de los cuerpos policiales y de inteligencia, también en la propia ciudadanía, se consideran

[369] ARROYO ROMERO, F.J., *La influencia de Europol en la comunitarización de la policía europea*, Ediciones Akal, 2006, p. 89.

[370] Por ejemplo, sobre las características y las tipologías delictivas.

como graves otras conductas delictivas que desbordan los marcos de la delincuencia organizada y el terrorismo. Ciertamente, no es una cuestión de fácil respuesta, ni mucho menos de fácil consenso entre los distintos Estados miembros y surgen dudas y preguntas *¿Cómo se establece el criterio de gravedad? ¿En función de si llevan asociada una pena de prisión o no? ¿En función de los años de prisión asociados a la condena? ¿En función del perjuicio causado a la víctima?* La sentencia por el caso planteado por la Audiencia Provincial de Tarragona no resuelve tampoco estas incógnitas y deja a la normativa y jurisprudencia de cada Estado miembro la determinación de la gravedad del delito y la forma de considerarlo. Sin conocer los debates concretos que tuvieron lugar en el seno del Consejo de la Unión Europea cuando se negoció el borrador final de la Directiva de Conservación de Datos, por la experiencia previa en este tipo de discusiones en el ámbito de las instituciones europeas, consideramos, sin temor a equivocarnos, que se pusieron sobre la mesa los diferentes criterios nacionales a la hora de fijar un umbral mínimo de lo que pudiera considerarse un delito grave y, teniendo en cuenta que una directiva establece un conjunto de reglas mínimas respecto de las que los Estados miembros pueden ser más restrictivos, finalmente se dejó redactado de una forma muy abierta, sin pensar en que este podría ser uno de los argumentos que un tribunal [como ocurrió con el TJUE, a pesar de *acabar* con la Directiva. Lo que parece indudable, de acuerdo con Oromí i Vall-Llovera (2020; 3), [371] es que el uso de la tecnología en la sociedad [y en la criminalidad] incide en la eficacia y la eficiencia de los procesos judiciales.

En la normativa europea relacionada con la privacidad y la protección de los datos se hace referencia a los delitos graves cuando se trata la limitación de los derechos y obligaciones; sin embargo, no se ha fijado de forma clara cómo se determina qué delitos son graves y en función de qué parámetros. Es decir, el Tribunal no aporta una definición del concepto de delito grave, como tampoco lo encontramos en la normativa y textos de cooperación judicial penal, adoptados en virtud del artículo 83 del TFUE. Sí podemos encontrar una definición en términos cuantitativos del concepto de delito grave en la Directiva sobre registro de nombres de los pasajeros (conocida como

[371] OROMÍ I VALL-LLOVERA, S., *"Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE"*, en Revista de los Estudios de Derecho y Ciencia Política, IDP nº. 31, 2020, pp. 1-13, p. 3.

Directiva PNR)[372], que remite a un anexo de la norma en la que se establece que estos serán los que conlleven una pena de privación de libertad con una duración máxima no inferior a tres años. En cambio, otra norma también muy posterior a la Directiva de Conservación de Datos, el Reglamento de Europol[373], define la delincuencia grave haciendo referencia a un listado de veintitrés delitos recogidos en un anexo.

En definitiva, ante la imprecisión del concepto y la necesidad de determinar la gravedad de un delito, recurrir a un concepto numérico quizás sea lo más adecuado o, como mínimo, el punto de partida de la discusión. Evidentemente, esto producirá discrepancias notables entre los Estados miembros, por cuanto sus tradiciones jurídicas diferentes han hecho que el umbral de la pena asociada a un determinado delito sea diferente. Como ilustración de esta diferencia, Bahamonde Blanco (2018; 5)[374] cita el caso de Dinamarca y el sistema de ese país a la hora de establecer las penas, bajo la concepción de que la dureza de estas no determina su eficacia contra la delincuencia y, como ejemplo clarificador cita a la pornografía infantil que, siendo un delito grave, está castigado con un año de prisión. En España, para que un juez autorice el acceso a datos conservados, respecto de la gravedad del delito -y en unión de otros criterios concretos- se debe tratar de delitos dolosos castigados con pena de hasta tres años de prisión o aquellos que se lleven a cabo a través de medios telemáticos.

A la hora de intentar delimitar el concepto de delito grave, por ser este uno de los que contempla el Tribunal para *permitir* la injerencia en los derechos fundamentales que venimos tratando, se pregunta de forma inteligente Oromí i Vall-Llovera (2020; 7) [375] si ¿significa esto que un juez solo puede autorizar la obtención de datos personales

[372] Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos de registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. OJ L 119, 4.5.2016, p. 132-149, en http://data.europa.eu/eli/dir/2016/681/oj

[373] 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. OJ L 135, 24.5.2016, p. 53-114, en http://data.europa.eu/eli/reg/2016/794/oj

[374] BAHAMONDE BLANCO, M., *"Medidas de investigación tecnológica a la luz de los Derechos Fundamentales, una cuestión pendiente",* en Diario La Ley, 2018, consultado en https://diarioley.laleynext.es/Content/Documento.aspx?params , p. 5 .

[375] OROMÍ I VALL-LLOVERA, S., *"Acceso a datos personales conservados por proveedores…", op. cit.* p. 7

conservados por los proveedores de servicios de telecomunicaciones cuando se está investigando un delito grave? Ya hemos visto que no es fácil determinar la gravedad de un delito. Y, además, hay muchos delitos en los que la mayoría de los Estados miembros podrían estar de acuerdo sobre su consideración de no graves, pero para cuya investigación se precisa igualmente de este tipo de datos conservados como elementos fundamentales [en ocasiones único] para su esclarecimiento y puesta a disposición judicial del presunto autor. Pues bien, el Tribunal europeo, en el apartado 57 de la Sentencia del *Caso Ministerio Fiscal* ha reconocido que la injerencia en los derechos fundamentales respecto de los que se suscitó la cuestión prejudicial no es grave y puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir delitos en general.

En los apartados siguientes de la misma sentencia se reconoce que se puede autorizar la petición de datos que no permitan extraer conclusiones precisas sobre la vida privada de las personas, por no suponer una injerencia grave en los artículos 7 y 8 de la Carta. Por tanto, entendemos que la falta de gravedad del delito no puede justificar, por sí sola, la no autorización judicial de estas diligencias en el ámbito de las investigaciones penales.

3.2 Período de conservación de los datos

En lo que se refiere al período exacto por el que los datos pueden ser retenidos, la Directiva preveía un margen entre seis y veinticuatro meses. A este respecto, las sentencias del TJUE encontraron que *"el artículo 6 de la Directiva 2006/24/CE exige que dichos datos se conserven durante un período mínimo de seis meses, sin que se haga ninguna distinción entre las categorías de datos establecidas en el artículo 5 de dicha Directiva en función de su posible utilidad para el objetivo perseguido o en función de las personas afectadas"*[376].

Teniendo en cuenta lo anterior, este margen tan amplio llevó a una gran variedad de transposiciones en los Estados miembros. Como confirmó el estudio de Europol, el

[376] Sentencia TJUE, de 8 de abril de 2014, *caso Digital Rights Ireland*, párrafo 63.

tiempo máximo de retención dentro de cada legislación nacional se fijó en un año en siete Estados miembros (Estonia, Grecia, Hungría, Polonia, Lituania, España y Reino Unido) y en seis meses en cinco países (Bulgaria, Chipre, República Checa, Lituania y Suecia). El máximo período de retención previsto de dos años se adoptó únicamente por Italia.

Sin embargo, el análisis concluyó también que algunas legislaciones nacionales distinguían entre diferentes períodos de conservación en función del servicio prestado. De forma particular para los participantes en el estudio:

- Italia distinguía entre telefonía fija y móvil (dos años); y acceso a Internet, telefonía a través de Internet y correo electrónico a través de Internet (un año). Además, para llamadas perdidas de teléfono se fijó un año, mientras que para datos de facturación y propósitos administrativos se reducía a un mes.
- Finlandia diferenciaba períodos de retención en función del tipo de servicio en sí mismo: servicio de teléfono o de SMS (un año), servicio de acceso a Internet (nueve meses) y servicio de teléfono a través de Internet (seis meses).
- En España, la ley de 2007 ha establecido un año. Sin embargo, tras consultar a los operadores, el período puede ser extendido o reducido para determinadas categorías de datos hasta un máximo de dos años o un mínimo de seis meses, en función del coste de almacenamiento y de los intereses a los efectos de la investigación del delito grave.
- En Bulgaria la obligación se fija en seis meses. Aun así, puede ser extendida por un período adicional de otros seis meses ante la solicitud de las autoridades policiales.

En definitiva, la determinación de la duración de la conservación, debido a la divergencia entre unos Estados miembros y otros, no parece haberse basado en criterios objetivos cuyo principio rector sea que este abarque lo estrictamente necesario o se adapte a circunstancias concretas, como pide el TJUE, aunque bien es cierto que hasta este momento las sentencias no dan pistas sobre qué considera el Tribunal que debiera

ser una duración adecuada de la conservación de los datos recogidos. En sentencias más recientes, que analizaremos a continuación, sí se precisa más sobre esta cuestión y podremos obtener otro tipo de conclusiones al respecto.

Otro apartado relevante sobre el que basó también su decisión el Tribunal europeo fue la correspondiente a las medidas de seguridad sobre los datos conservados, para evitar manipulaciones o accesos indebidos, además de robos. La Directiva invalidada no establecía normas específicas para proteger la ingente cantidad de datos que los proveedores de servicios habían de conservar, ni se diferenciaba entre unos y otros datos según su sensibilidad. Por el contrario, quizás por la presión del sector, que no estaba de acuerdo con los costes que deberían asumir para cumplir con las previsiones de la norma europea, se concedió la potestad a las empresas para establecer el nivel de seguridad sobre los datos en función de aspectos económicos. Es lógico pensar que, ante esta prerrogativa, la mayoría de ellas optarían por un sistema de mínimos en cuanto a la seguridad de los datos, lo que no garantizaba que no pudieran ser explotados con fines distintos a los previstos por la norma. También cuestionó el Tribunal que no se impusieran obligaciones de conservación en el territorio de la Unión y se confiara esa importante labor de custodia a empresas ubicadas en *demarcaciones* en las que no se dispone de una normativa tan exigente con la protección de los datos personales. Recordemos, a modo de ejemplo, aunque muy importante, la sentencia citada en otros apartados de este estudio, por la que se invalidó el régimen de transferencia de datos entre la UE y los EE. UU; pues bien, podemos imaginar fácilmente otros países con mayor probabilidad de que los datos transferidos sean tratados con menores garantías que en EE. UU y a los que la propia Directiva no impedía recurrir para su custodia. En definitiva, el Tribunal de Luxemburgo observó que la normativa invalidada debía haber previsto mayores controles y exhibir un mayor rigor sobre los datos conservados, exigiendo su conservación en territorio de la UE y adoptando medidas de seguridad adicionales y complementarias a las acciones empresariales de custodia de estos.

3.3 El dilema del cifrado de las comunicaciones

El cifrado de las comunicaciones también juega un papel importante en el debate sobre la retención de datos de las comunicaciones electrónicas. En este aspecto concreto, el Tribunal afirma que *"…. la Directiva 2006/24/CE no contiene garantías suficientes, como las que exige el artículo 8 de la Carta, que permitan asegurar una protección eficaz de los datos conservados contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos respecto de tales datos…"*[377]. El riesgo de abuso al que se refiere el Tribunal podría ser limitado mediante el uso de medidas técnicas apropiadas como es el cifrado o la *"anonimización o enmascaramiento*[378]*"*, como prescriben varias normas europeas de protección de datos[379]; por ejemplo, el considerando 60 de la Directiva (EU) 2016/680[380] establece que *"el responsable o encargado del tratamiento debe evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado"*.

Adicionalmente, el Tribunal objetó también la falta de obligaciones que se imponen a los operadores, argumentando que la Directiva *"… no garantiza que dichos proveedores apliquen un nivel especialmente elevado de protección y seguridad mediante medidas técnicas y organizativas…"*[381].

La encuesta de Europol evidenció que la mayoría de los países participantes tienen en sus respectivos sistemas legales obligaciones que establecen que los datos conservados necesitan ser cifrados, para la protección tanto de la integridad como de la confidencialidad de la información que contiene. Además, en la fase de intercambio de información, una cantidad significativa de Estados miembros cifra los datos antes de

[377] Sentencia TJUE, de 8 de abril de 2014, *caso Digital Rights Ireland*, párrafo 66.

[378] No se abordarán con detalle en el estudio las técnicas de enmascaramiento disponibles, como la *"anonimización"* y *"seudoanonimización"*, entre otras, por su carácter muy técnico y completo, que lo alargaría innecesariamente.

[379] Entre otras, Art. 6.4 (e), Art. 32.1(a), Art. 34.3(a) del Reglamento (EU) 2016/679 (General de Protección de Datos) y Art. 32 y Art. 33 del Reglamento (EU) 2016/794 (Reglamento de Europol).

[380] Directiva (UE) 2016/680, 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 (Directiva Policía).

[381] Sentencia TJUE, de 8 de abril de 2014, *caso Digital Rights Ireland*, párrafo 67.

transferirlos, independientemente de que la información se entregue a otros organismos nacionales o a autoridades extranjeras.

A pesar de ello, el cifrado no sólo es importante cuando se trata de proteger los datos conservados, sino que constituye también un reto en el contexto de la investigación de delitos graves y de terrorismo. Los desafíos que presenta encontrar un equilibrio adecuado entre el derecho a la privacidad y, al mismo tiempo, otorgar a las fuerzas de seguridad los medios adecuados para investigar los delitos, se debatieron durante una conferencia sobre *"La privacidad en la era digital del cifrado y el anonimato en línea"* celebrada en la sede de Europol, los días 19 y 20 de mayo de 2017[382]. La conferencia contó con la participación de diferentes organizaciones públicas y privadas, con el SEPD, la Autoridad Común de Control de Europol, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea -ENISA-, Eurojust, Amnistía Internacional y otros muchos actores de una amplia gama de ámbitos profesionales, en representación de la industria privada, el mundo académico, los defensores de la privacidad y las fuerzas de orden.

Hubo consenso general en que la disponibilidad y el uso de tecnologías de cifrado y anonimato no sólo son importantes y legítimos en muchas circunstancias, sino que son esenciales para un ciberespacio seguro. Otro de los temas principales de la conferencia versó sobre la dicotomía que el cifrado y el anonimato en línea suponen para las fuerzas de orden para proteger a los ciudadanos de comportamientos delictivos y extremistas, y para llevar a los responsables ante la justicia. Como destacó el entonces director de Europol, el Sr. Wainwright:

> *"los retos para las fuerzas del orden son muy reales y suponen una pérdida de oportunidades de investigación como consecuencia del creciente uso indebido de los servicios y herramientas legítimos de anonimato y cifrado con fines ilegales. Para las fuerzas del orden, por tanto, el aspecto clave es definir las*

[382] No se ha tenido acceso al documento de conclusiones del encuentro, solo a determinados elementos de debate y algunas ideas fuerza que se debatieron entre los expertos . Consideramos que no hay objeción en reflejarlos en nuestro estudio, por no desvelar información sensible ni clasificada.

modalidades de acceso legal, dentro de unos límites bien definidos y regulados, respetando plenamente los derechos fundamentales".

Haciéndose eco de la necesidad de unos límites bien definidos y regulados, el director de ENISA, Sr. Helmbrecht, aconsejó:

"no debilitar el cifrado a propósito; no inhibir el uso de herramientas para la protección de datos y la privacidad: promover la seguridad de las Tecnologías de la Información. La legislación apresurada suele ser inadecuada, hay que dar tiempo para debatir e invertir en I+D".

El acto ofreció buena oportunidad para mantener un debate abierto entre diferentes puntos de vista, con el fin de encontrar una forma de mejorar la seguridad en línea sin sacrificar la Libertad, aunque, a nuestro juicio se pedía compaginar dos realidades de difícil *mezcla* y que requiere seguir un *largo y tortuoso camino* para conseguirlo. Al final de la conferencia, los directores de ambas agencias europeas emitieron una declaración conjunta en la que describen los retos y se proponen posibles vías de solución para las investigaciones penales legales que respeten la protección de datos del siglo XXI.

3.4 Colaboración entre las fuerzas de seguridad y los servicios de inteligencia

Los datos conservados también desempeñan un importante papel cuando se trata de la colaboración entre las fuerzas de seguridad y los servicios de inteligencia. Desde el punto de vista de su protección, cualquier colaboración de este tipo es delicada, porque las condiciones y los requisitos para obtener el acceso a ellos suelen ser muy diferentes. Esto, combinado con las acusaciones de *Edward Snowden* sobre la vigilancia masiva[383] en 2013, llevó al Comité LIBE[384] del Parlamento Europeo a celebrar más de

[383] Analiza PERALTA GUTIÉRREZ (2021) el estado de la cuestión (la vigilancia masiva) en relación con las sentencias Quadrature du Net y Big Brother Watch -que analizaremos- y arguye que "cada vez se escucha más la posibilidad de una regulación europea de la vigilancia masiva en el camino hacia una NSA o CIA europea". No obstante, veremos a lo largo del estudio que los indicadores actuales no apuntan hacia esa vía de salida. Para profundizar sobre los argumentos del autor, vid. PERALTA GUTIÉRREZ, A, "La necesaria regulación de la vigilancia masiva: Casos Quadrature du Net y Big

15 audiencias, teniendo en cuenta las presentaciones de expertos de la Unión Europea y de los Estados Unidos, las instituciones de la UE, e incluso las ramas legislativas del gobierno de los Estados Unidos[385].

De vuelta una vez más a la encuesta de Europol, esta puso de manifiesto que, *"teniendo en cuenta la posible confusión entre los servicios de inteligencia y los cuerpos de seguridad, solo unos pocos Estados miembros observaron ocasionalmente un solapamiento entre sus acciones"*, principalmente en relación con el intercambio de mejores prácticas o la participación conjunta dentro del ciclo de inteligencia. Sin embargo, en lo que respecta a las normas aplicadas en el mismo, la gran mayoría de los Estados miembros confirmaron que las competencias y limitaciones específicas -incluidas las relativas a los datos retenidos- están explícitamente organizadas y aplicadas por medio de la legislación, los acuerdos interinstitucionales y el intercambio mutuo de funcionarios en comisión de servicio.

Cabe señalar que, en este contexto, la Autoridad Común de Supervisión de Europol llevó a cabo una inspección extraordinaria en septiembre de 2014, provocada por una convocatoria del Parlamento Europeo. El objetivo de la inspección era determinar si la información y los datos personales compartidos por Europol habían sido obtenidos legalmente por las autoridades nacionales y, en particular, si fueron adquiridos inicialmente por los servicios de inteligencia. Europol se sintió satisfecha al ver que la Autoridad Común de Supervisión no encontró ninguna información que indicara que los datos se habían obtenido violando los derechos fundamentales o sin respetar la legislación nacional de los Estados contribuyentes o de las organizaciones internacionales. Además, la Autoridad Común confirmó también que Europol cuenta

---

Brother Watch", Diario La Ley, nº. 9973, 2021, en https://diariolaley.laleynext.es/dll/2021/12/17/la-necesaria-regulacion-de-la-vigilancia-masiva-casos-quadrature-du-net-y-big-brother-watch

[384] Comité de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) es una de las Comisiones del Parlamento Europeo, que se encarga de los asuntos legislativos y políticos de mayor relevancia para los ciudadanos europeos en el ámbito de la libertad, seguridad y justicia, según establece el artículo 3 del TUE. Ver https://www.europarl.europa.eu/committees/es/libe/about).

[385] Ver la web, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN, consultada el 17.08.21.

con medidas de procedimiento bien establecidas para garantizar que se comprueba la conformidad de los datos entrantes antes de introducirlos en sus sistemas[386].

3.5 Reacciones de algunos Estados miembros a las sentencias del TJUE

Hemos hecho referencia a que algunos Tribunales constitucionales nacionales[387], antes de la sentencia de 2014 se pronunciaron sobre la constitucionalidad de sus leyes de transposición de la Directiva europea de Conservación de Datos, declarando algunos de ellos no ajustado a derecho total o parcialmente esas leyes nacionales. De hecho, el TJUE recoge algunas de esas críticas en sus sentencias. A pesar de ello, los Altos tribunales nacionales pueden seguir un criterio diferente al europeo y, de hecho, todavía hoy lo hacen [recordemos el caso español].

Recoge Rizzo (2019; 304)[388] algunos ejemplos concretos de Estados miembros que adoptaron acciones inmediatas tras la publicación de la primera de las sentencias [otros tras la de 2016 y otros están aún en proceso de aprobación de nuevas normativas nacionales]:

- *Reino Unido* hizo una lectura favorable a los intereses de los cuerpos policiales y de inteligencia y consideró que su normativa nacional puede seguir aplicándose si existen salvaguardas adecuadas.
- *Bélgica* vio invalidada su normativa por el Tribunal Constitucional en 2015 y adoptó otra norma en 2016, diferenciando entre delitos menores y graves en cuanto al periodo de conservación de los datos (6 meses y 9 ampliable a 12, respectivamente).
- En *Alemania* se declaró inconstitucional la norma por no cumplir con el principio de proporcionalidad. En este sentido, es interesante señalar que no consideró inconstitucional el almacenamiento en sí mismo, sino la falta de medidas de seguridad de los datos y el que no se impusieran restricciones al acceso. Se aprobó una nueva ley en 2015, que establecía diferentes periodos

[386] http://www.europoljsb.europa.eu/media7267640/1441%20final%20data%20inspection%20report%20september%202014-%20v07.pdf, consultada el 12 de agosto de 2021.

[387] Bulgaria en 2008, Rumanía en 2009, Alemania en 2010 y Chipre y la República Checa en 2011.

[388] RIZZO, G., *"El derecho a la privacidad y…", op. cit.*, pp. 304 y ss.

de conservación en función de los tipos de datos, exigiendo la destrucción de todos ellos de forma rápida pasada el plazo máximo de retención.

- *España*, como hemos analizado, sigue manteniendo la 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[389] y, respecto del período de conservación de los datos -por comparación con los países anteriores- establece un máximo de 12 meses, aunque puede ser aumentado hasta el límite superior establecido por la Directiva de 2006 (2 años) o reducido al mínimo que contempla (6 meses) en función de los costes asociados a los proveedores de servicios. En definitiva, se tuvieron en cuenta los intereses de las empresas afectadas más que los de los cuerpos policiales.
- *Italia* ha mantenido también su legislación, con los tiempos de conservación más amplios que permite la Directiva.
- *Eslovenia y Austria* suspendieron la aplicación de sus legislaciones nacionales hasta que se dictara sentencia en el caso Digital Rights Ireland y, en base a esta, anularon sus normas.

En resumen, cada Estado miembro de los mencionados [y es de suponer que el resto ha hecho lo mismo] han optado por soluciones diferenciadas que, como argumenta Rizzo (2019; 309)[390], tienen que ver con la perspectiva de la soberanía: *"siempre que la ley y la jurisprudencia lo permitan, los Estados miembros tienen interés en interpretar los derechos fundamentales en la forma en que les deja el margen máximo para poner en práctica sus políticas.* Y, de acuerdo en parte con este autor, esta disputa forma parte, como hemos venido defendiendo aquí, de *"la diferencia entre países respecto de los paradigmas de seguridad"*. No podemos estar tan de acuerdo cuando asevera que *"los tribunales toman en serio la idea de que las restricciones de derechos deben limitarse a lo estrictamente necesario incluso cuando las restricciones se justifican por la seguridad, mientras que los gobiernos parecen considerar las salvaguardias legales de los derechos fundamentales como un tecnicismo que debe aplicarse, pero de la manera que menos interfiera con el objetivo de la política de seguridad".* Este aserto no deja de

[389] Vid. https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243
[390] RIZZO, G., *"Derecho a la privacidad…"*, op. cit., p. 309.

confirmar más que cada uno de los poderes de un estado desempeña su papel constitucional de la mejor forma posible y, como hemos defendido, el que haya que buscar un cierto equilibrio en un asunto que no ha encontrado solución hasta ahora, no quiere decir que uno y otro no se *lo tomen en serio*. De hecho, hemos visto que ciertos Tribunales nacionales se han posicionado del lado de la interpretación que los gobiernos han hecho respecto de sus normativas nacionales, aun cuando el Tribunal europeo había fijado un criterio claro y contundente a través de las sucesivas sentencias sobre la Directiva de Conservación de Datos de 2006.

4. Nuevos pronunciamientos a cuestiones prejudiciales

4.1 Sentencias de octubre de 2020

Posteriormente, se presentaron otras peticiones de decisión prejudicial por el Tribunal de Competencias de Investigación del Reino Unido (*Investigatory Powers Tribunal*)[391], el Tribunal Constitucional de Bélgica[392], el Consejo de Estado (*Conseil d'État*) de Francia[393] y el Tribunal Supremo de Estonia[394].

En sus sentencias de 6 de octubre de 2020, el Tribunal confirmó una vez más su doctrina anterior[395] en el sentido de que los datos de las comunicaciones electrónicas son confidenciales y no pueden conservarse de manera generalizada e indiscriminada. En este caso, el TJUE establece excepciones limitadas a este principio en relación con la

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

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

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

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

[395] Sentencia TJUE, de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12; sentencia de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15.

seguridad nacional, la defensa y la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos, que hacen que de nuevo se despierte optimismo e interés en los expertos que estaban analizando el problema, desde hace ya demasiados años, y buscando posibles vías de solución compatibles con los intereses de todas las partes involucradas.

4.1.1 Casos acumulados C-511/18, C-512/18 *"La Quadrature du Net et al./Ordre des barreaux francophones et germanophone et al."*

En esta sentencia, el TJUE sienta doctrina respecto a cómo interpretar el artículo 15, apartado 1 de la Directiva de privacidad electrónica y con qué límites, estableciendo los supuestos y situaciones tasados en los que puede tener cabida a los efectos que venimos estudiando, pero se reafirma en que la norma general es su incompatibilidad con el Derecho de la Unión, como ya había hecho en las sentencias de 2014 y 2016. Mantiene también su jurisprudencia anterior en la decisión preliminar de 6 de octubre de 2020 al recapitular que *"el Derecho de la Unión Europea se opone a una legislación nacional que obligue a un proveedor de servicios de comunicaciones electrónicas a realizar la transmisión o conservación general e indiscriminada de datos de tráfico y de localización con el fin de luchar contra la delincuencia en general o de salvaguardar la seguridad nacional como medida preventiva"*.

Sin embargo, al mismo tiempo, también como en ocasiones anteriores, aclara que *"los Estados miembros pueden adoptar medidas legislativas que prevean la conservación de datos durante un período limitado si son necesarias, adecuadas y proporcionadas en una sociedad democrática para salvaguardar la seguridad nacional, la defensa y la seguridad pública, así como la prevención, la investigación, la detección y la persecución de delitos o del uso no autorizado del sistema de comunicaciones electrónicas"*[396] (apartado 110).

[396] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 110.

Hay una cuestión que sigue quedando meridianamente clara: el almacenamiento de los datos debe ser una excepción. No puede convertirse en la norma[397] (apartado 111).

En el apartado 132, el Tribunal confirmó también que, para cumplir el requisito de proporcionalidad, la legislación debe:

a) *"Establecer normas claras y precisas sobre el alcance y la aplicación de la medida en cuestión y prever garantías mínimas",*
b) *Ser jurídicamente vinculante y específica en la legislación nacional,*
c) *Concretar las circunstancias y condiciones bajo las que una medida que permita el tratamiento de dichos datos pueda ser tomada, y*
d) *Limitarse a lo estrictamente necesario*[398].

En este contexto, nos centraremos en aquello que se *permite*, pues es ahí donde se deberán buscar las posibles soluciones y los puntos de encuentro que equilibren los intereses enfrentados:

- *Medidas legislativas que prevén la conservación preventiva de los datos de tráfico y de localización con el fin de salvaguardar la seguridad nacional*[399]

El Tribunal subrayó que el artículo 4, apartado 2, del Tratado de la Unión Europea establece que la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro. Esto corresponde, entre otras cosas, a la prevención y al castigo de actividades capaces de desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país y, en particular, de amenazar directamente a la sociedad, a la población o al propio Estado, como las actividades terroristas[400] (TUE, 2010; C 83/18).

[397] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 111.

[398] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net* , apartado 132.

[399] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 134 y ss.

[400] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net* , apartado135.

En situaciones en las que un Estado miembro se enfrenta a una amenaza grave para la seguridad nacional que se demuestra que es real y presente o previsible, *"el Derecho de la UE no se opone a que se recurra a una orden que exija a los proveedores de servicios de comunicaciones electrónicas que retengan, de forma general e indiscriminada, los datos de tráfico y los datos de localización de todos los usuarios de los sistemas de comunicaciones electrónicas durante un período de tiempo limitado"*[401] (apartado 137).

Esta conservación preventiva de datos debe limitarse en el tiempo a lo estrictamente necesario. Además, debe estar sujeta a limitaciones y afectada por salvaguardas estrictas que permitan proteger eficazmente los datos personales contra el riesgo de abuso. La conservación *"renovable"* no debe ser sistemática[402] (apartado 138).

Las decisiones que dan instrucciones a los proveedores para llevar a cabo la conservación de datos deben estar sujetas a una revisión efectiva por parte de un tribunal o de un organismo administrativo independiente cuya decisión sea vinculante[403] (apartado 139).

- *Medidas legislativas que prevén la retención preventiva de datos de tráfico y de localización con el fin de luchar contra la delincuencia grave y salvaguardar la seguridad pública -conservación selectiva[404] (apartados 140 y ss.).*

El Tribunal dictaminó que el Derecho de la UE no se opone a la conservación selectiva de datos de tráfico y de localización. Esto significa que la retención restringida a las personas afectadas o a determinadas zonas geográficas, sobre la base de factores

[401] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 137.

[402] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 138.

[403], Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 139.

[404] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 140 y ss.

objetivos y no discriminatorios, está permitida con el fin de salvaguardar la seguridad nacional, luchar contra la delincuencia grave y prevenir las amenazas graves para la seguridad pública, siempre que el período se limite a lo estrictamente necesario[405] (apartados 144 y 147). A pesar de ello, no pueden conservarse de forma sistemática y continua[406] (apartado 142).

- *Medidas legislativas que prevén la conservación preventiva de las direcciones IP como parte de los datos de tráfico[407] (apartados 152 y ss.).*

El Tribunal confirma que el Derecho de la UE no se opone a las medidas legislativas que prevén la conservación generalizada e indiscriminada de las direcciones IP asignadas al origen de la comunicación, siempre que el período de conservación se limite a lo estrictamente necesario.

Considera que las direcciones IP no revelan en sí mismas ninguna información sobre terceros que hayan estado en contacto con la persona que realizó la comunicación, y declara que las direcciones IP son menos sensibles que otros datos de tráfico. A pesar de ello, dado que pueden utilizarse para rastrear toda la actividad en línea de un usuario de internet, los datos permiten elaborar un perfil detallado del usuario[408] (apartado 152).

Reconoce también que, cuando se comete un delito en línea, la dirección IP puede ser el único medio que permita la investigación de la persona a la que se asignó. Además, esos datos no son necesarios para los proveedores a los efectos de facturación de los servicios que ofrecen[409] (apartado 154).

[405] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 144;147.

[406] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 142.

[407] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net* apartados 152 y ss.

[408] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 152.

[409] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 154.

Por lo tanto, la obligación de conservación preventiva de estas para luchar contra la delincuencia grave, prevenir amenazas graves para la seguridad pública y salvaguardar la seguridad nacional puede estar justificada, siempre que el período de conservación no exceda de lo estrictamente necesario a la luz del objetivo perseguido[410] (apartado 156).

- *Medidas legislativas que prevén la conservación preventiva de datos relativos a la identidad civil*[411] (Apartado 157).

El Derecho de la UE no se opone a las medidas legislativas que prevén, a los mismos fines, la conservación general e indiscriminada de los datos relativos a la identidad civil de los usuarios y abonados. En particular, los Estados miembros no están obligados en este último caso a limitar el período de conservación[412] (apartado 159).

- *Medidas legislativas que prevén la conservación mediante un procedimiento abreviado*[413] *de los datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave*[414] *(apartados 160 y ss.).*

El Derecho de la Unión no se opone a una medida legislativa que permita recurrir a la conservación acelerada de los datos de que disponen los proveedores de servicios, cuando se produzcan situaciones en las que sea necesario conservar esos datos más allá de los plazos legales de conservación de datos en caso de delitos graves o de atentados contra la seguridad nacional, cuando dichos delitos o atentados ya se hayan cometido o cuando pueda sospecharse su existencia[415] (apartado 164).

---

[410] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 156.

[411] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 157.

[412] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 159.

[413] *"Expedited"* en inglés.

[414] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 160 y ss.

[415] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 164.

En estas situaciones, se permite que los Estados miembros prevean la posibilidad de ordenar, mediante una decisión de la autoridad competente sujeta a control judicial efectivo, la retención acelerada o abreviada de los datos de tráfico y localización de que dispongan durante un periodo de tiempo determinado. La injerencia, una vez más, ha de limitarse a lo estrictamente necesario, aunque esa duración puede ampliarse[416] (apartados 163 y ss.). La retención no tiene que limitarse necesariamente a los datos de personas sospechosas, sin o que puede ampliarse a otras personas relacionadas directa o indirectamente con la investigada.[417] (apartado 165).

- *Análisis automatizado de datos de tráfico y localización*[418] (apartados 172 y ss.).

El TJUE aclara que el análisis automatizado de estos datos solo pasa la prueba de proporcionalidad en aquellas situaciones en las que un Estado miembro se enfrenta a una amenaza grave para la seguridad nacional, *"en particular para prevenir el terrorismo, que se demuestra que es real y presente o previsible. Además, la duración de dicha retención debe limitarse a lo estrictamente necesario y ha de estar sujeta a una revisión efectiva"*[419] (apartados 177 a 179). Los modelos y criterios preestablecidos para decidir que se está en una situación con las descritas deben ser específicos y fiables[420] (apartado 180).

- *Recogida en tiempo real de datos de tráfico y localización*[421] *(apartados 183 y ss.)*

El Alto Tribunal afirma que las medidas que se adopten deberán estar sujetas a una *"revisión previa"* realizada por un tribunal o por un organismo administrativo

[416] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 163 y ss.
[417] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 165.
[418] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 172 y ss.
[419] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 177 a 179.
[420] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 180.
[421] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 183 y ss.

independiente cuya decisión sea vinculante *"para garantizar que dicha recogida en tiempo real sólo se autorice dentro de los límites de lo estrictamente necesario"*[422] (apartados 188 y ss.).

Por tanto, mediante esta sentencia se sientan las bases de la futura conservación de datos de las comunicaciones electrónicas, al enumerar de forma exclusiva y excluyente los supuestos que puedan dar lugar a posibilitar la conservación generalizada e indiferenciada que declaró contraria a derecho en la Directiva 2006/24/CE, además de todas las garantías que deberán acompañar a esta retención; y de aquellos supuestos para los que las medidas deberán ser selectivas y/o susceptibles de una intervención acelerada o rápida. De hecho, podemos considerar que establece una excepción a su doctrina anterior, permitiendo a los Estados miembros adoptar las medidas a través de los proveedores de servicios de telecomunicaciones en casos considerados como *excepcionales*.

Algunos autores, como expone Polo Roca (2021;12)[423], temen que con este criterio matizado del Tribunal de Luxemburgo se esté avalando la vuelta a un régimen de conservación de datos de forma preventiva[424]. Aun así, no está de acuerdo con ello, como tampoco lo estamos nosotros, sino que, al contrario, considera [consideramos] que perjudica el mantenimiento de la Ley 25/2007, de transposición de la Directiva de 2006, debido a las exigencias que el Tribunal fija en el *Caso La Quadrature du Net* y otros. En este punto, creemos conveniente recordar que, en la fecha de redacción del presente trabajo, la norma española sigue aplicándose y el Tribunal Supremo ha avalado su vigencia, por lo que entendemos que el debate parte de que esta norma debería ser derogada de acuerdo con el pronunciamiento ya en 2016 del Tribunal de Justicia europeo, en la Sentencia del *Caso Tele2 Sverige.* Así lo entendía también Colomer Hernández (2018; 78)[425] quien considera que, a partir de esa sentencia, la ley española

[422] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 188 y ss.

[423] POLO ROCA, A., *"La regulación sobre la conservación de datos…", op. cit.*, p.12.

[424] Vid. RODRÍGUEZ LAINZ, J.L. (2020), *"El renacer de la Ley Española sobre conservación de datos relativos a las comunicaciones"* (Comentario a la STJUE, Gran Sala, de 6 de octubre de 2020). Diario La Ley, nº. 9740

[425] COLOMER HERNÁNDEZ, I., *"La cesión de datos de las comunicaciones electrónicas para su uso en investigaciones criminales: una problemática en ciernes"*, en JIMÉNEZ CONDE, F.J (dir.),

de 2007 no puede amparar la cesión de esos datos para la investigación penal, ni siquiera con autorización judicial.

Nos detendremos en los argumentos que el Tribunal Supremo establece en su razonamiento para justificar que las deficiencias de las que adolecía la Directiva europea no tienen cabida en el ordenamiento jurídico español y, en consecuencia, la refrenda y concluye que rechaza plantear una cuestión prejudicial ante la instancia europea por *"entender que la Ley 25/2007, valorada en su globalidad, es respetuosa con el derecho de la Unión Europea y que, en todo caso, la eventual lesión del derecho al secreto de las comunicaciones y del resto de derechos fundamentales afectados por el régimen de conservación y cesión de datos debe hacerse analizando las circunstancias del caso concreto, determinando si la incorporación de los datos al proceso judicial ha sido proporcionada, necesaria y sometida al principio de contradicción"* (Sentencia del TS 727/2020, de 23 de marzo de 2001)[426]. A mayor abundamiento, para el caso concreto objeto de valoración por el TS, considera que el soporte legal de los datos conservados se apoya también en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y que *"los datos que se cedieron eran susceptibles de conservación no sólo por razones de seguridad pública sino por otras*

Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales. Valencia, Tirant lo Blanch, 2018, pp. 77-100, p. 78.

[426] STS 727/2020, de 23 de marzo de 2021, recurso de casación núm. 4218/2018, en https://vlex.es/vid/864876864. *"En la sentencia 22/2018, de 31 de julio de 2018, dictada por la Audiencia Provincial de Cuenca en el Procedimiento Abreviado 148/2012, se presenta recurso por los condenados, denunciando que la Ley 25/2007, de 18 de octubre, que sirvió de soporte jurídico a la captación de los datos de tráfico de varios números de teléfono y que fue la diligencia inicial de la investigación de los hechos enjuiciados, es contraria al derecho de la Unión Europea y lesiona varios derechos fundamentales, por lo que la conservación y la posterior cesión de esos datos a la autoridad judicial adolecen de nulidad radical y deben dar lugar a la nulidad no sólo de esa prueba sino de las restantes pruebas que tienen su origen en la captación ilegal. Se alega también que la obtención de datos de tráfico almacenados por las compañías de teléfono fue posible por la existencia de una régimen legal que ordena su conservación de modo indiscriminado, hasta el punto de que todas las comunicaciones electrónicas o telefónicas, con cualquier clase de dispositivo, en cualquier lugar de España, efectuadas por cualquier persona y por cualquier motivo, quedan registradas y almacenadas durante el período, no precisamente breve, establecido en la Ley 25/2007, de 18 de octubre, que es de un año. Dicho régimen de conservación masiva e indiferenciada es contrario a la interpretación del derecho a la privacidad y a la protección de datos establecida por el Tribunal de Justicia de la Unión Europea en su sentencia de 21 de diciembre de 2016, caso Tele 2. Teniendo en cuenta la primacía del derecho de la Unión Europea sobre el nacional y que la interpretación de los derechos fundamentales se debe hacer de conformidad con los tratados internacionales ratificados por España, la consecuencia de la doctrina del TJUE es que los datos recogidos en virtud de un régimen legal como el español lo fueron mediante la violación de un derecho constitucional, en especial el consagrado en el artículo 18.4, pero también en el 18.1, de ahí que la prueba en cuestión sea nula y también lo sean las restantes pruebas de cargo que derivan directamente de la conservación ilegal de los datos de tráfico".* (Fundamentos de derecho 1.1)

razones estrictamente comerciales y su cesión a la autoridad era obligada con independencia de lo dispuesto por la Ley 25/2007, de conformidad con lo dispuesto en la Ley de Enjuiciamiento Criminal"[427]. Esto es especialmente relevante, por cuanto, las cuestiones prejudiciales planteadas por otras instancias nacionales ante el TJUE se han fundamentado de forma similar y finalmente han resultado en una confirmación del Tribunal europeo de su doctrina anterior. Estamos de acuerdo con Tomás Mallén (2017; 479)[428] acerca de que *"la ejecución de sentencias del TJUE, como parte del más amplio cumplimiento de las obligaciones comunitarias europeas, no sólo reviste complejidad jurídica, sino que además tiene un indudable impacto político y económico"*. La reticencia del Alto tribunal español a asumir la invalidez de la normativa nacional de transposición de la Directiva de 2006 da fe de esa dificultad; el hecho de que se siga aplicando –aun cuando el juez o tribunal tenga que valorar caso por caso la validez de las pruebas- está teniendo ya consecuencias políticas y las tendrá también económicas, puesto que pronosticamos que el final será la invalidación también de la norma española y podría provocar medidas de compensación. Creemos que, aunque el TS rechace [por el momento] plantear una cuestión prejudicial, este criterio puede variar a medida que surjan otros pronunciamientos de Luxemburgo que impidan mantener la doctrina de los Estados miembros; en este caso, de España. Reseñaremos a continuación algunos de los fundamentos que han llevado al TS a conformar su criterio.

No considera que la invalidación de la Directiva 2006/24/CE suponga automáticamente la anulación de la norma española. La Directiva europea fue declarada nula por un conjunto de carencias o deficiencias que, en su conjunto, la convertían en laxa y producía la ausencia de protección suficiente sobre determinados derechos de los afectados. Considera el TS que, si se realiza el mismo análisis sobre la Ley 25/2007, gran parte de esas deficiencias no se observan, puesto que:

- la ley española obliga a la conservación de datos de tráfico y localización durante un año y permite su cesión a las autoridades judiciales, si bien esa cesión está sujeta a estrictas garantías;
- los prestadores de servicios obligados por la ley a la conservación de datos no pueden realizar operación alguna de tratamiento, a salvo de la cesión

[427] Artículo 579 derogado y actual artículo 588 ter j.
[428] TOMÁS MALLÉN, B., *"La ejecución de sentencias del Tribunal de Justicia…",* op. cit. 479.

singularizada que pueda recabar la autoridad judicial. Concede importancia a este hecho, ya que la doctrina del TJUE ha tenido como finalidad esencial la protección de los derechos a la vida privada, a la protección de datos y a la libertad de expresión, hasta el punto de que en sus sentencias se ha insistido en que los datos conservados, *"... considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado ..."* En cambio, argumenta el TS que la ley española no genera ese riesgo, ya que los datos conservados permanecen custodiados y no pueden tener más uso que su cesión a la autoridad judicial cuando lo ordene bajo un riguroso sistema de garantías;

- sólo cabe ceder los datos conservados para la detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes especiales, que actualmente requiere acudir al artículo 579.1 de la LECrim, que sólo autoriza este tipo de injerencias en delitos castigados con al menos pena de prisión de 3 años, en delitos de terrorismo y en delitos cometidos por grupos u organizaciones criminales;
- los datos que deben ser conservados son los necesarios para rastrear e identificar el origen y destino de una comunicación, el tipo de comunicación y el equipo de comunicación de los usuarios, pero en ningún caso se pueden conservar datos que revelen el contenido de la comunicación;
- los datos sólo pueden ser cedidos previa autorización y resolución judicial que autorice la cesión deberá ser motivada y ajustarse a los principios de necesidad y proporcionalidad, especificando los datos que han de ser cedidos. Considera el TS que esta garantía es esencial y muchas de las legislaciones de los Estado miembros autorizaban la cesión a autoridades no judiciales;
- la cesión se limita a su utilización en investigaciones penales por delitos graves y no cabe la conservación o cesión para finalidades distintas de la investigación penal, como, según el TS, ha ocurrido en otras legislaciones; ni para la investigación de delitos de escasa entidad;
- los datos sólo pueden ser cedidos a agentes facultados, señalando como tales a los miembros de las Fuerzas y Cuerpos de Seguridad, Agentes de Vigilancia Aduanera y agentes del CNI, y deberán limitarse a la información imprescindible;

- la ley impone a los sujetos obligados todo un conjunto de obligaciones para garantizar la integridad, seguridad, calidad y confidencialidad de los datos y establece un régimen de sanciones;
- la LECrim ha realizado una completa regulación de las intervenciones telefónicas y telemáticas, incluyendo en ellas el uso de los datos conservados por obligación legal, sujetando todas ellas a un estricto control judicial en su adopción y en su ejecución, con aplicación de los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad.

Por tanto, concluye el TS que muchos de los déficits de normatividad de la Directiva anulada por el TJUE no se dan en el ordenamiento legal español al establecer garantías suficientes para que los datos personales conservados por obligación legal estén suficientemente protegidos frente al riesgo de abuso ilegal tanto en relación con el acceso a esos datos como en el uso de estos. Y esa es la razón para la que la Sala del TS había considerado también en ocasiones anteriores[429] que el ordenamiento español en materia de conservación y cesión de datos es conforme con el derecho de la Unión.

Analiza también el Alto tribunal español los efectos de esta cuestión en el proceso penal concreto y se pronuncia en el siguiente sentido: *"la legislación española en su conjunto es respetuosa con los derechos reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea, de ahí que nuestro análisis se proyecte no tanto en cómo debe regularse en el futuro esta materia, como en la comprobación de que en cada proceso penal y respecto de todo ciudadano que se vea sometido a una investigación criminal tenga la garantía del pleno respeto de sus derechos constitucionales. El propio TJUE ha situado en ese punto la proyección práctica de su doctrina. Lo determinante a efectos del proceso penal es si la limitación que sufre cada investigado en sus derechos fundamentales supone una injerencia no respetuosa con la Carta de Derechos Fundamentales de la Unión Europea y, en general, con los derechos fundamentales reconocidos en nuestra Constitución"*.

[429] STS 723/2018, de 23 de enero de 2019 y 400/2017, de 1 de junio; dictadas a la vista de las STJUE de 2014 y 2016.

4.1.2 Caso C-623/17 "Privacy International"

En esta sentencia, el Tribunal europeo subrayó que la legislación nacional que permite a una autoridad estatal exigir *"a los proveedores de servicios de comunicaciones electrónicas que transmitan los datos de tráfico y de localización a los organismos de seguridad e inteligencia con el fin de proteger la seguridad nacional entra en el ámbito de aplicación de la Directiva 2002/58/CE"*[430] (apartado 41). Por lo tanto, bajo la aplicación del artículo 15, apartado 1 de la Directiva de privacidad electrónica, están la conservación, el acceso y la transmisión que, como ha quedado más que acreditado, suponen diferentes niveles de injerencia en los derechos fundamentales de los ciudadanos europeos.

En relación con lo anterior, también dictaminó que el Derecho de la Unión debe interpretarse en el sentido de que se opone a una legislación nacional que permita a una autoridad estatal exigir a los proveedores que realicen la transmisión general e indiscriminada de datos de tráfico y de localización a los organismos *"de seguridad e inteligencia con el fin de salvaguardar la seguridad nacional"*[431], ya que ello excede los límites de lo estrictamente necesario y no puede considerarse justificado en una sociedad democrática[432], faltando con ello a la debida ponderación que recoge el artículo 51, apartado 1 de la Carta de los Derechos Fundamentales de la Unión Europea.

4.2 Sentencia de marzo de 2021

La sentencia del 2 de marzo del pasado año, en el *asunto C-746/18 H.K v. Prokuratuur*[433], si bien mantiene también la jurisprudencia anterior en cuanto al acceso de las autoridades nacionales a los datos relativos a las comunicaciones electrónicas, aporta algunas novedades que requieren también de análisis.

El Tribunal reafirma, una vez más, que el Derecho de la Unión Europea se opone a las medidas legislativas que prevén, con carácter preventivo, la conservación

[430] Sentencia TJUE, de 6 de octubre de 2020, *Privacy International*, apartado 41.
[431] Sentencia TJUE, de 6 de octubre de 2020, *Privacy International*, apartados 81 y siguiente.
[432] Sentencia TJUE, de 6 de octubre de 2020, *Privacy International*, apartado 81.
[433] Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, H.K. v. Prokuratuur.

general e indiscriminada de datos; es decir, no limitadas a las categorías específicas de delitos graves[434] (apartado 30).

Respecto del objeto de nuestro análisis, reitera los requisitos que debe cumplir cualquier norma legislativa sobre conservación de datos para cumplir con el principio de proporcionalidad, es decir: reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, y que indique las circunstancias y requisitos para el tratamiento de los datos.

De la misma forma, también se mantiene en su tesis respecto de que las medidas legislativas destinadas al tratamiento de los datos de identificación civil de los usuarios de medios de comunicación electrónica, como su conservación y acceso con el único fin de identificarlos (sin que los datos estén asociados a la información relativa a las comunicaciones realizadas) pueden estar justificadas por el objetivo de la prevención, investigación, detección y persecución de las infracciones penales en general, en la medida en que:

> *"tales datos no permiten por sí mismos conocer la fecha, la hora, la duración y los destinatarios de las comunicaciones efectuadas, ni los lugares en los que se produjeron dichas comunicaciones, ni la frecuencia de las mismas con determinadas personas durante un período determinado, y, por tanto, no aportan ninguna información sobre las comunicaciones efectuadas ni sobre su vida privada, la injerencia causada por la conservación de estos datos de identificación civil no puede calificarse de grave"*[435] (apartado 34).

Por otra parte, el Tribunal de Justicia mantiene el criterio de que es esencial que el acceso de las autoridades nacionales sea objeto de un control previo por parte de un

[434] Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, H.K. v. Prokuratuur, apartado 30.

[435] Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, H.K. v. Prokuratuur, apartado 34.

órgano jurisdiccional/administrativo independiente y que la decisión debe adoptarse tras una solicitud motivada[436] (apartado 51).

En ese sentido, establece que el control previo exige que el órgano jurisdiccional/administrativo encargado de llevarlo a cabo disponga de las competencias y garantías necesarias para asegurar la conciliación de los distintos intereses en juego. En la investigación penal, el control exige que el órgano jurisdiccional o la entidad estén en condiciones de garantizar un justo equilibrio entre los intereses vinculados a las necesidades de la investigación en materia de lucha contra la delincuencia y los derechos fundamentales relacionados con el respeto de la vida privada y la protección de los datos personales, actuando con objetividad e imparcialidad[437] (apartado 52).

Considera que la exigencia de independencia que impone el control previo implica que, cuando el control no es efectuado por un órgano jurisdiccional, sino por un órgano administrativo independiente, este debe gozar de un estatuto que le permita actuar de manera objetiva e imparcial en el ejercicio de sus funciones y, a tal efecto, debe estar libre de toda influencia externa. De esto se desprende que debe ser un tercero en relación con la autoridad que solicita el acceso a los datos y no debe participar en la realización de la investigación penal en cuestión, sino que ha de ostentar una posición neutral frente a las partes del procedimiento penal[438] (apartado 53).

Por lo tanto, el Tribunal determinó que no puede ser el ministerio público (ministerio fiscal) quien lleve a cabo la investigación y ejerza también el poder de decisión con total independencia, sino que ha de ser sometido, en su caso, a la consideración de un tribunal competente, como parte en el proceso penal. El hecho de que el fiscal esté obligado, en virtud de las normas que regulan sus competencias y su estatuto, a verificar los elementos incriminatorios y exculpatorios, a garantizar la

[436] Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, H.K. v. Prokuratuur, apartado 51.

[437] Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, H.K. v. Prokuratuur, apartado 52.

[438] Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, H.K. v. Prokuratuur, apartados 53 y 54.

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

Lo cierto es que, a la luz de los pronunciamientos del Tribunal de Justicia de la Unión Europea, ha ido creando y matizando su doctrina sobre la conservación de datos personales en el ámbito de las telecomunicaciones, a través de sentencias de los años 2014 y 2016, y las más recientes de 2020 y 2021, pero es palmario que ha fijado de nítidamente un criterio general que subyace a todos sus pronunciamientos, cual es: el Derecho de la Unión Europea se opone a una conservación generalizada e indiscriminada/indiferenciada de todos los datos de las comunicaciones electrónicas y para todo *momento y lugar*, y ello tanto para normativa europea como, tras la sentencia de 2016 [a pesar de que no todos los Estados miembros han dejado de aplicar sus normativas nacionales], para las normativas nacionales de los Estados miembros.

5. Más dudas, mismas respuestas

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

El 5 de abril pasado (2022) se publica una nueva sentencia de la Gran Sala del Tribunal[439], en este caso respecto de una cuestión prejudicial planteada por el Tribunal Supremo de Irlanda (C-140/20) mediante resolución de 25 de marzo de 2020. De nuevo Irlanda solicita el parecer del de Luxemburgo (como ya lo hizo sobre la Directiva 2006/24/CE), pero esta vez respecto de un proceso civil dirigido a solicitar la invalidez de determinadas disposiciones de su normativa nacional de transposición de la Directiva de conservación de datos (aprobada mediante una ley de 2011). En esta ocasión, anulada la Directiva de 2006, se pretendía confrontar la ley nacional con la habilitación prevista en el artículo 15, apartado 1 de la Directiva europea de privacidad electrónica de 2002.

[439] Sentencia TJUE (Gran Sala), de 5 de abril de 2022, caso *Commissioner of the Garda Síochána y otros*, en el asunto C-140/20.

Aunque el TJUE ha venido reiterando su doctrina en las sucesivas sentencias, el tribunal irlandés alberga todavía dudas sobre las exigencias del Derecho de la Unión respecto de la conservación de datos con fines de lucha contra la delincuencia y argumenta que *"solo una conservación generalizada e indiferenciada de los datos de tráfico y de localización permite luchar eficazmente contra la delincuencia grave y que, en cambio, una conservación selectiva y una conservación rápida (quick freeze) no resultarían tan eficaces"*. Además, respecto de la conservación selectiva, cuestiona la posibilidad de centrarse en grupos o zonas geográficas determinados a efectos de la lucha contra la delincuencia grave, *"en la medida en que ciertos delitos graves rara vez implican circunstancias que las autoridades nacionales competentes conozcan y que les permita sospechar con anticipación la comisión de un delito, además de que una conservación selectiva pueda dar lugar a discriminaciones. En cuanto a la conservación rápida, considera que solo es útil en situaciones en las que existe un sospechoso que puede ser identificado en una fase temprana de la investigación"* (apartado 26). Observamos sintonía plena entre los argumentos y dudas que traslada el tribunal irlandés y los manifestados por la mayoría de los expertos que en el ámbito del Consejo de la Unión Europea en las discusiones que comenzaron hace más de un lustro y que trasladan el sentir de las autoridades policiales y también algunas judiciales [no quiere decir que haya habido voces críticas entre las autoridades judiciales que se han pronunciado en esas reuniones, sino que no todas ellas lo han hecho, como sí ha ocurrido de forma casi unánime entre las policiales] a nivel de los Estados miembros.

En esta sentencia, el Tribunal reitera lo que ya dijo un año antes, en la conocida como *La Quadrature du Net y otros*, respecto de que la conservación de datos de tráfico y de localización constituye una excepción a la prohibición establecida en el artículo 5, apartado 1, de la Directiva 2002/58/CE, siendo irrelevante 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 debido a tal injerencia (apartado 44). El Tribunal incide, una vez más, en que no se opone a medidas legislativas que permitan, a efectos de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan 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 enfrenta a una amenaza grave

para la seguridad nacional que resulte real o previsible (apartado 58). Reitera también que, respecto de la prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave y la prevención de las amenazas graves contra la seguridad pública pueden justificar las injerencias graves en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, como las que supone la conservación de los datos de tráfico y de los datos de localización. Eso sí, solo las injerencias que no presenten un carácter grave pueden estar justificadas por el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general (apartado 59). En ese sentido, vemos que la propia Comisión Europea también está alineada con la posición del Consejo y de las Estados miembros en esta materia y, como refleja la reciente sentencia: *"la Comisión Europea sostuvo que la delincuencia especialmente grave podría asimilarse a una amenaza para la seguridad nacional"*. Es ciertamente un debate interesante y difícil, no abordado en este estudio, pero que podría dar lugar a un trabajo específico. Aunque el TJUE ha cerrado el debate para el objeto de nuestro estudio -la conservación de datos de telecomunicaciones a los efectos de la lucha contra la delincuencia grave-, creemos que podría aportar elementos interesantes a la discusión respecto de la compleja relación entre Libertad y Seguridad.

En ese sentido, aclara el Tribunal europeo que el objetivo de la seguridad nacional (para diferenciarlo de la delincuencia grave) corresponde *"al interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad e incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado, tales como las actividades terroristas"*[440] (apartado 61). Cita expresamente al terrorismo como fenómeno que, a través de sus actividades de terror, pueden llegar a poner en peligro las estructuras fundamentales de un estado. Parece que en esto no hay grandes desacuerdos, como sí los hay cuando nos referimos a la delincuencia grave. Si centramos el análisis en la Unión Europea, por suerte, la delincuencia organizada grave no parece tener capacidad de llegar hasta ese nivel de amenaza a nuestras sociedades. Si miramos a

[440] Como también lo había ya indicado el propio Tribunal en la Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 135.

otras zonas geográficas del mundo, esa afirmación no parece tan contundente. Obviamente, el régimen de conservación de datos se creó para operar en la Unión Europea, pero la evolución de las amenazas en un mundo como el actual, debido entre otras causas a tensiones geopolíticas constantes y que afectan directamente a áreas geográficas enormemente alejadas del lugar en el que se producen o la supresión de las fronteras que han permitido las tecnologías de las comunicaciones y de la información, y la internacionalización de los delitos, podrían llegar a aproximar las actividades del crimen organizado y transnacional con el de las actividades del terror, hasta el punto de que las primeras también puedan poner en peligro de forma grave las estructuras fundamentales de determinadas sociedades democráticas.

En el apartado 62, ahonda más en las diferencias entre ambos fenómenos [contestando a la argumentación de la Comisión Europea], señalando que las amenazas para la seguridad nacional deben ser reales y actuales, o al menos previsibles y, por tanto, deben emerger *"circunstancias suficientemente concretas para poder justificar una medida de conservación generalizada e indiferenciada de datos de tráfico y de localización, durante un plazo limitado"*. Continúa diciendo que, *"así pues, tal amenaza se distingue, por su naturaleza, su gravedad y el carácter específico de las circunstancias que la forman y del riesgo general y permanente de que surjan tensiones o perturbaciones, incluso graves, que afecten a la seguridad pública o del riesgo de delitos graves"*[441]. Entiende y defiende el Tribunal, por tanto, que no procede considerarlas asimilables y, en esta misma idea se pronunció también el Abogado General[442] al afirmar que *"tal asimilación podría implicar la introducción de una categoría intermedia entre la seguridad nacional y la seguridad pública para aplicar a la segunda las exigencias inherentes a la primera"*.

Refuta también el Tribunal el argumento expresado anteriormente, respecto de que solo una conservación generalizada e indiferenciada de estos datos permitiría luchar de forma eficaz contra la delincuencia grave, arguyendo que *"la eficacia de las acciones penales depende generalmente no de un solo medio de investigación, sino de*

[441] También recogido en la Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 136 y 137.

[442] Conclusiones del Abogado General de la Unión Europea en el Caso C-140/20

todos los medios de investigación que se hallen a disposición de las autoridades nacionales competentes a los referidos efectos". Estamos de acuerdo con este razonamiento, aunque es un argumento general que, como hemos señalado en diferentes ocasiones, se ha visto cada vez más limitado precisamente como una consecuencia de la evolución tecnológica, y es algo que, a pesar de las diferencias en cuanto a los medios y técnicas de investigación (además también de la diferente legislación penal entre países) entre las agencias encargadas de la aplicación de la ley en los diferentes Estados miembros europeos, ha concitado las mismas reacciones de alarma ante la invalidación de la Directiva de 2006 y las sucesivas sentencias del Alto tribunal de Luxemburgo. Esta unanimidad en el diagnóstico parece querer indicar que los servicios policiales y de investigación deben buscar soluciones más imaginativas y no centrar sus pesquisas tanto en las posibilidades que ofrece este tipo de datos. Ya hemos citado, de forma somera, algunos casos concretos en los que la falta de acceso y uso de esta información impide progresar en la investigación y, en consecuencia, hace fracasar la acción penal sobre delincuentes (hoy también sobre terroristas) que han conculcado derechos fundamentales de ciudadanos europeos.

Parece querer también el Tribunal explicar que ha diferenciado entre categorías de datos y que no se ha opuesto a la conservación general e indiferenciada de algunos de ellos, como los datos relativos a la identidad civil y, en ese contexto, cita un ejemplo concreto en el que estas acciones generales se pueden llevar a cabo a nivel nacional (en aquellos Estados miembros que así lo han regulado): el control documental de la identidad, y su registro, de aquellas personas que adquieran una tarjeta SIM de prepago; información que debe cotejar y recoger el vendedor, y poner a disposición de las autoridades nacionales competentes, si es requerido para ello[443]. Quizás siendo consciente el Tribunal de que se le está interrogando sobre las mismas cuestiones y que la reiteración de su doctrina (aunque con pequeños matices) no es suficiente, aporta algún ejemplo concreto más para justificar su reiterado posicionamiento anterior que permita ofrecer algunas excepciones a la invalidación total del régimen de conservación de datos instaurado por la Directiva de 2006. En ese sentido, cita una vez más la posibilidad de conservar de forma general e indiferenciada las direcciones IP atribuidas al origen de una conexión (apartado 74), así como que respecto de la conservación

[443] En España se reguló esta obligación a raíz de los atentados del 11 de marzo en Madrid.

selectiva y/o rápida de datos, la Carta *"no sujeta la posibilidad de expedir un requerimiento que imponga una conservación selectiva al requisito de que se conozcan de antemano los lugares que pueden ser escenario de un acto delictivo grave ni las personas sospechosas de estar implicadas en tal acto. De igual forma, dicha Directiva no exige que el requerimiento que impone una conservación rápida se limite a los sospechosos que ya habían sido antes identificados"* (apartado 75). También aporta otros criterios para la conservación selectiva, siempre que esté permitido por el derecho nacional, no impidiendo que las medidas se proyecten sobre *"personas a las que se identifica porque están siendo investigadas o están siendo objeto de otras medidas de vigilancia o constan en el registro nacional de antecedentes penales por una condena anterior por delitos graves que puedan implicar un elevado riesgo de reincidencia"* (apartado 78).

Otro argumento cuestionado por los Estados miembros, y esgrimido también en la cuestión prejudicial que motiva esta sentencia, es la dificultad para establecer un criterio geográfico a la hora de solicitar una conservación selectiva de metadatos. En ese sentido, el Tribunal también aporta un ejemplo concreto de posible criterio que justifique tal medida: la tasa media de delincuencia en una zona geográfica, aunque no se cuente con indicios concretos sobre la preparación o la comisión de delitos graves en esas zonas concretas (apartado 80). Para llevar a cabo este análisis permanente y dinámico, como para otros de los criterios apuntados por el Tribunal, al margen de la necesidad de recursos policiales y judiciales disponibles [creemos que su ausencia y/o coste adicional no serían argumentos suficientes para justificar que no se puedan poner en práctica], la aplicación de este criterio trasladará una carga de trabajo adicional elevada y su correspondiente coste en recursos humanos, medios técnicos y tecnológicos; y de seguridad, para los proveedores de servicios, que sin duda no estarán dispuestos a asumir de buen grado.

A lo anterior, el Tribunal añade de forma expresa una referencia a que las autoridades de los Estados miembros asuman su responsabilidad en la identificación de otros criterios, dejándose entrever un mensaje implícito, como decíamos antes, respecto de que estos adolecen de falta de imaginación en la búsqueda de soluciones y, quizás

también, una mera resistencia al cambio ante una situación que se ha considerado no ajustada a Derecho. Al menos, a nuestro entender este es el mensaje que se desprende de la lectura del punto 50 de las Conclusiones del Abogado General, que también recoge el apartado 83 de la reciente sentencia: *"la eventual existencia de dificultades para definir con precisión los casos y las condiciones en que pueda realizarse una conservación selectiva no justifica que los Estados miembros, haciendo de la excepción una norma, establezcan una conservación generalizada e indiferenciada de datos de tráfico y de localización"*.

Respecto de la conservación rápida *(quick freeze)*, también aporta nuevos elementos que pretenden precisar más las posibilidades de uso de esta técnica de conservación al servicio de la investigación de delitos graves. En ese sentido, precisa que *"no es imprescindible que se adopte respecto de personas identificadas previamente como representativas de una amenaza para la seguridad pública o la seguridad nacional del Estado miembro de que se trate o de personas de las que se sospecha que han cometido un delito grave o un atentado contra la seguridad nacional"* (apartado 88). Al contrario, esta puede ampliarse a personas distintas de las sospechosas, e incluso podría ser autorizada respecto de las *"personas con las que haya estado en contacto una víctima al utilizar los medios de comunicaciones electrónicas de aquellos antes de que se produjera una amenaza grave para la seguridad pública o de que se cometiera un delito grave"* (apartado 89) o, respecto de criterios geográficos, al lugar en el que una víctima potencial de un delito grave haya desparecido; todo ello desde la primera fase de la investigación (apartado 91). Empero, por muy temprana que sea esa fase, consideramos que en la investigación de muchos delitos será tardía y se perderá la posibilidad de analizar el histórico de esos mismos datos y, con ello, una pieza fundamental en la que basar el curso inicial de las pesquisas.

Por otro lado, responde el Tribunal en parte a la duda que planteamos en el primer capítulo de la tesis, respecto del difícil [para algunos autores, casi imposible] equilibrio entre Libertad y Seguridad y la ponderación de las medidas para garantizar ambos derechos o conjunto de derechos fundamentales. En ese sentido, como hizo también en su sentencia de octubre de 2020, considera que:

"ni siquiera las obligaciones positivas de los Estados miembros que pueden resultar, según el caso, de los artículos 3, 4 y 7 de la Carta[444] *y que se refieren, como ha señalado en el apartado 49*[445] *de la presente sentencia, a la adopción de normas que permitan combatir eficazmente los delitos, pueden tener por efecto justificar injerencias tan graves, como las que supone una normativa que establece una conservación de los datos de tráfico y de localización, en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta de prácticamente toda la población sin que los datos de las personas afectadas puedan guardar una relación, al menos indirecta, con el objetivo perseguido"* (apartado 95).

Otra cuestión importante también suscitada (en este caso por el gobierno danés) es la relativa a la posibilidad de que las autoridades nacionales puedan acceder, a efectos de la lucha contra la delincuencia grave, a los metadatos conservados para hacer frente a una amenaza grave a la seguridad nacional que resulte real y actual o previsible y que, en consecuencia, hayan dado lugar a una conservación general e indiferenciada. Una vez más, se observa una dinámica de consulta al Tribunal, de forma reiterada, cuestionando la posibilidad de incardinar en su doctrina determinadas medidas que permitan ampliar las posibilidades de investigación a los efectos de la lucha contra la delincuencia grave. No obstante, también una vez más, el TJUE mantiene su posicionamiento y, así, considera que lo que se está proponiendo es autorizar el acceso de unos metadatos que han sido conservados con un objetivo concreto (una amenaza grave para la seguridad nacional de un Estado miembro) para otro fin distinto (la lucha contra la delincuencia grave) y, por tanto, dependiendo de unas circunstancias ajenas a aquel objetivo. Concluye el Tribunal diciendo que: *"solo cabría una solución diferente si la importancia del objetivo perseguido fuera mayor que la del objetivo que justificó*

[444] Artículo 3, 4 y 7 de la Carta de los Derechos Fundamentales de la Unión Europea, relativos respectivamente a: derecho a la integridad de la persona; prohibición de la tortura y de las penas o los tratos inhumanos o degradantes; y respeto de la vida privada y familiar.

[445] Apartado 49 de la Sentencia, de 6 de octubre de 2020, caso *La Quadrature du Net* y otros, en el Caso C-140/20: *"De esta manera, por lo que respecta, específicamente, a la lucha efectiva contra los delitos perpetrados, en particular, contra los menores y otras personas vulnerables, debe tenerse en cuenta que del artículo 7 de la Carta pueden resultar obligaciones positivas que incumban a los poderes públicos, con miras a la adopción de medidas jurídicas dirigidas a proteger la vida privada y familiar. Estas obligaciones pueden resultar asimismo de dicho artículo 7 por lo que se refiere a la protección del domicilio y de las comunicaciones, así como de los artículos 3 y 4 en lo tocante a la protección de la integridad física y psíquica de la persona y a la prohibición de la tortura y de los tratos inhumanos o degradantes"*, apartado 126 y jurisprudencia citada.

la conservación" (apartado 98) y, para el caso concreto presentado por el gobierno danés, cree el Tribunal que *"autorizar, en tal situación, el acceso a los datos conservados sería contrario a la jerarquía de objetivos de interés general sugerida en el apartado anterior [98] y en los apartados 53, 56, 57 y 59*[446] *de la presente sentencia"* (apartado 99).

En conclusión, una vez más, el TJUE mantiene su doctrina anterior y confirma que el artículo 15, apartado 1 de la Directiva 2002/58/CE [ante la declaración de nulidad de la Directiva 2006/24/CE es el que habilita a los Estados miembros a adoptar medidas de conservación de datos de telecomunicaciones] se opone a medidas legislativas que establezcan, con carácter preventivo, a los efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización. No se opone a que se establezcan otro tipo de medidas que ya recogió en sentencias anteriores. En definitiva, la conclusión general, con determinados matices concretos que hemos ido desgranando, es la misma que ante cuestiones prejudiciales planteadas por los mismos u otros países y por motivos relacionados. Para Rodríguez Laínz (2022)[447] a la luz de esta sentencia, se acrecienta la urgencia respecto de la necesidad de adaptación de la legislación española y la jurisprudencia en la materia a las exigencias del Tribunal. Considera el autor que *"el gran mérito de la sentencia no será sino esa primera grieta*

[446] Referidos a la determinación de la gravedad de la injerencia que supone la limitación de derechos y la importancia del objetivo de interés general perseguido por dicha limitación en relación con tal gravedad; la existencia de una jerarquía entre dichos objetivos en función de su importancia respectiva y que la importancia del objetivo perseguido por tal medida debe ser correlativa a la gravedad de la injerencia que supone la medida; que la importancia de la protección de la seguridad nacional, supera la de los demás objetivos contemplado en el artículo 15, apartado 1 de la Directiva 2002/58/CE, en particular los objetivos de combatir la delincuencia en general, incluso grave, y de protección de la seguridad pública y, en consecuencia, puede justificar medidas que supongan injerencias en los derechos fundamentales más graves que las que podrían justificar esos otros objetivos; y a que solo la lucha contra la delincuencia grave y la prevención de las amenazas graves contra la seguridad pública pueden justificar las injerencias graves en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta y, en consecuencia, solo las injerencias en tales derechos fundamentales que no presenten un carácter grave pueden estar justificadas por el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general.

[447] RODRÍGUEZ LAÍNZ, J.L., *"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 Commissioner an Garda Síochána",* Diario La Ley, nº. 10058, Sección Tribuna, 2022, en https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAmNTI2MDI7Wy1KLizPw8WyMDIyMDE0NLtbz8lNQQF2fb0ryU1LTMvNQUkJLMtEqX_OSQyoJU27TEnOJUtdSk_PxsFJPiYSYAAGi40aZjAAAAWKE

que se aprecia en el hasta entonces inexpugnable muro de la radical oposición a cualquier forma de régimen legal de conservación preventiva de datos" y cree encontrar la justificación en *"la apreciación [por el Tribunal] del escasísimo nivel de injerencia que pudiera derivarse de su sola recopilación preventiva, así como el considerar que tales datos llegan a ser indispensables para evitar que reinara la más absoluta impunidad en las redes de comunicaciones electrónicas"*. Es cierto que se abren vías más claras para perfilar el *nuevo* régimen de conservación, pero no observamos que el cambio sea tan *radical* como el que expone el profesor.

Una novedad de esta sentencia respecto a las anteriores es el pronunciamiento sobre qué autoridades están habilitadas para conceder la autorización para acceder a los datos conservados, refiriéndose de forma particular a las autoridades administrativas independientes. En la sentencia del *Caso Ministerio Fiscal*, cuestionó la independencia de los fiscales, por ser en muchos países los encargados de impulsar las investigaciones penales [esto no es aplicable a España]. En este caso concreto, se le interroga acerca de si un miembro de la Policía con funciones exclusivas para analizar las solicitudes y decidir sobre ellas, apoyado en una unidad concreta y especializada, cumple o no con los criterios de independencia exigidos. Para ese caso concreto y con las circunstancias concretas presentadas por Irlanda, el TJUE considera que el artículo 15, apartado 1 de la Directiva en cuestión se opone a que esta labor la realice un funcionario de policía, puesto que *"no tiene la calidad de tercero con respecto a esos servicios, no cumple las exigencias de independencia e imparcialidad mencionados en el apartado 108*[448] *de la presente sentencia, pese a la circunstancia de estar asistido en esa función por una unidad de la Policía, [..], que goza de cierto grado de autonomía en el ejercicio de sus funciones"* (apartado 111).

[448] El apartado 108 de la sentencia recuerda el principio de primacía del Derecho de la Unión sobre el de los Estados miembros. De acuerdo con , dice el Tribunal que: *"cuando no resulte posible interpretar la normativa nacional conforme a las exigencias del Derecho de la Unión, el juez nacional encargado de aplicar, en el ámbito de su competencia, las disposiciones del Derecho de la Unión tendrá la obligación de garantizar la plena eficacia de estas, dejando inaplicada si fuera necesario, y por su propia iniciativa, cualquier disposición contraria de la legislación nacional, aun posterior, sin que deba solicitar o esperar su previa eliminación por vía legislativa o mediante cualquier otro procedimiento constitucional"* (véase en ese sentido, las sentencias de 15 de julio de 1964, Costa, 6/64, EU:C:1964:66, pp. 105 y 106; de 19 de noviembre de 2019; A.K. y otros (Independencia de la Sala Disciplinaria del Tribunal Supremo), C-585/18, C-624/18 y C-625/18, EU:C:2019:982, apartados 157, 158 y 160, así como 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 214 y 215).

Por último, se requiere también del Tribunal un pronunciamiento respecto de si *"un órgano jurisdiccional nacional puede limitar en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, en virtud del derecho nacional, con respecto a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en razón de la incompatibilidad de dicha normativa con el artículo 15, apartado 1, de la Directiva 2002/58/CE a la vista de la Carta"* (apartado 115)[449]. Para ello, el Tribunal comienza recordando que corresponde al juez penal nacional el examen de la admisibilidad de las pruebas basadas en esos datos (de acuerdo con el principio de autonomía procesal) y también, una vez más, el principio de primacía del Derecho de la Unión sobre el de los Estados miembros, al que ya nos referimos antes. En ese sentido, en el apartado 119, el Tribunal relata que sólo él, con carácter excepcional y en atención a consideraciones imperiosas de seguridad jurídica, puede suspender el efecto de exclusión que ejerce una norma de la Unión sobre el Derecho nacional contrario a ella y solo puede admitirse en la propia sentencia que resuelve sobre la interpretación solicitada por el tribunal nacional. Concluye que el órgano jurisdiccional no puede limitar en el tiempo los efectos de una declaración de invalidez. Revela López Escudero (2019; 82)[450] que, si bien la primacía y el efecto directo han sido dos principios fundamentales que han establecido las relaciones entre el Derecho de la Unión y los nacionales, en su jurisprudencia más reciente el TJUE ha modulado esta doctrina y ha admitido límites al respecto, entre ellos, *"la ausencia de efecto directo de normas de la UE sobre la ausencia de obligación del juez nacional de inaplicar normas internas contrarias a directivas invocadas en relaciones horizontales"*; con el que no está de acuerdo.

En el apartado 122 recoge una consideración que, a nuestro entender, pone fin al debate sobre la validez de las leyes nacionales de transposición de la Directiva 2006/24/CE: *"En efecto, el mantenimiento de los efectos de una normativa nacional*

[449] La ley nacional a la que se está refiriendo es la Ley de 2011, de Irlanda, que se adoptó en transposición de la Directiva 2006/24/CE de Conservación de datos de las comunicaciones electrónicas.

[450] LÓPEZ ESCUDERO, M., *"Primacía del Derecho de la Unión Europea y sus límites en la jurisprudencia reciente del TJUE",* Revista de Derecho Comunitario Europeo, 64, 2019, pp. 787-825, p. 822.

como la Ley de 2011 [ley nacional irlandesa] *significaría que dicha normativa sigue imponiendo a los proveedores de servicios de comunicaciones electrónicas obligaciones que son contrarias al Derecho de la Unión y que suponen injerencias graves en los derechos fundamentales de las personas cuyos datos se han conservado"*[451]. Esta lapidaria aseveración del Tribunal europeo, a nuestro entender, supone definitivamente el final de todas aquellas normas nacionales derivadas de la Directiva 2006/24/CE en aplicación y, no deja dudas de que, si la norma española se llevara ante la instancia europea, aunque haya sido avalada por nuestro Tribunal Supremo, es más que probable que también provoque una sentencia desfavorable para España. En consecuencia, no se debería dejar pasar más tiempo en la búsqueda de una solución que adelante este escenario, por los efectos perjudiciales y graves sobre los derechos de los ciudadanos y, no menos importante, por la dificultad que se añadiría al trabajo policial y judicial, a partir del momento de esa eventual sentencia desfavorable y con efectos directos sobre cada uno de los procesos judiciales en curso. Es cierto que los pronunciamientos del Tribunal de Luxemburgo se producen habitualmente varios años después de recurrir, pero ante un criterio monolítico que suma ya varias sentencias, no debería mantenerse durante más tiempo una situación como la actual.

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

La última sentencia[452] [publicada en el momento en que se estaba llegando al final de nuestra investigación], resuelve una cuestión prejudicial del Tribunal Supremo de lo Contencioso-Administrativo de Alemania en sendos procedimientos en que empresas de telecomunicaciones germanas (SpaceNet y Telekom Deutschland) recurrieron ante sus tribunales nacionales la obligación que les impone la Ley de Telecomunicaciones de ese país[453] para la conservación general e indiferenciada de los datos de tráfico y localización de las comunicaciones electrónicas de sus clientes, desde el 1 de julio de 2017 y durante plazos limitados[454].

[451] Vid., por analogía, Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*; apartado 219.

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

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

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

La norma alemana se aprobó en 2004, por tanto, también en transposición de la Directiva de 2006. El Tribunal Constitucional alemán había declarado nula la legislación anterior, por lo que la ley se modificó en diciembre de 2015 para adaptarse al dictamen del Alto Tribunal alemán. Ese es el motivo por el que actualmente recoge algunas características que la diferencian de las de otros Estados miembros. Consideramos que precisamente esas diferencias son las que han hecho albergar dudas al Tribunal Supremo alemán, ya que parece indicar que, a priori, podían ser suficientes para no conculcar los preceptos de la Directiva 2002/58/CE ni provocar una injerencia *inadmisible* en los derechos fundamentales afectados por la materia, de los que gozan los ciudadanos alemanes mediante el uso de los servicios de voz e Internet en sus comunicaciones electrónicas.

El Tribunal alemán recurrente dice ser consciente de que el europeo ya ha declarado que las normativas de conservación de datos de tráfico y de localización, así como el acceso a ellos por las autoridades nacionales, están comprendidas en el ámbito de aplicación de la Directiva de 2002 [habida cuenta de la invalidación de la Directiva de 2006] y, en consecuencia, conoce que las medidas que se adopten habrán de estar justificadas en base al artículo 15, apartado 1 de esa norma europea. Aquí no observamos elemento novedoso alguno, salvo que el Tribunal alemán alberga dudas razonables sobre si la legislación nacional cumple o no ese criterio. Para ello, detalla las diferencias que observa en la ley alemana respecto de aquellas otras que han sido ya objeto de pronunciamiento, presentadas, entre otros estados, por Irlanda, Suecia o Francia:

- No se exige la conservación de todos los datos de tráfico relativos a las telecomunicaciones de todos los abonados y usuarios registrados en lo que respecta a todos los medios de comunicación electrónica. Excluye los datos relativos a los sitios de Internet consultados, los datos de los servicios de correo electrónico y los datos en los que se basan las comunicaciones de carácter social

o religioso hacia o a partir de determinadas líneas, que no podrán conservarse (apartado 32)[455].

- Establece un período de conservación muy inferior al de la mayoría de los Estados miembros y al que posibilitaba la Directiva de 2006[456]: cuatro semanas para los datos de localización y diez semanas para los datos de tráfico (apartado 33).
- Establece limitaciones estrictas en lo que respecta a la protección de los datos conservados y al acceso a ellos, de tal forma que, según el Tribunal alemán, garantiza una protección eficaz de los datos conservados frente a los riesgos de abuso y de acceso ilícito y, por otro, garantiza que su utilización solo podrá serlo para la lucha contra los delitos graves o para la prevención de un riesgo concreto para la integridad física, la vida o la libertad de una persona o para la existencia del Estado federal o de un *Land* (apartado 35)[457].

Otro tipo de consideraciones del Tribunal alemán, al margen de las diferencias materiales de la ley nacional suscitada respecto de las de otros Estados miembros; en este caso, sobre la interpretación de los derechos fundamentales afectados, son las siguientes:

- La incompatibilidad general con el Derecho de la Unión de toda conservación de datos sin motivo puede contravenir la obligación de actuar de los Estados miembros derivada del derecho a la seguridad consagrado en el artículo 6 de la Carta. Esta consideración, insistimos, nos parece muy pertinente, pues vemos en ella uno de los elementos centrales de todo debate posterior. Como indicábamos al comienzo de nuestro estudio, es un debate permanente y recurrente cada vez que surge un conflicto entre derechos (apartado 36)[458].
- También se plantea la cuestión sobre la capacidad de actuación de los Estados miembros ante materias que, según el artículo 4 del TUE, son responsabilidad exclusiva de los estados, como son la represión de los delitos y la seguridad

[455] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 32.

[456] La Directiva 2006/24/CE establecía un período de conservación entre seis meses y dos años.

[457] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 35.

[458] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 36.

pública (apartado 37). Esta es otra materia que hemos abordado previamente y que no solo nos genera dudas a nosotros, sino que algunos Estados miembros todavía hoy encuentran puntos de fricción con el criterio de la instancia judicial europea[459].

- Pone de manifiesto el Tribunal alemán que el TEDH *"ha declarado que el artículo 8 del CEDH no se opone a disposiciones nacionales que prevean la interceptación masiva de los flujos transfronterizos de datos, habida cuenta de las amenazas a las que se enfrentan actualmente muchos Estados y de las herramientas tecnológicas en las que pueden apoyarse en la actualidad terroristas y delincuentes para cometer actos reprobables"* (apartado 38). Nos parece también muy oportuna esta precisión para conocer el criterio del Tribunal europeo respecto de la relación [sobre la que incidimos en los capítulos iniciales de la tesis] entre el Tribunal Europeo de Derechos Humanos y el Tribunal de Justicia de la Unión Europea sobre la aplicación del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[460].

En este procedimiento se acumularon los casos C-793/19 y C-794/19, pero se acordó su suspensión por estar en una fase más avanzada la resolución del asunto que se sustanció con la *Sentencia La Quadrature du Net y otros* (C-511/18, C-512/18 y C-520/18). De hecho, numerosos argumentos de esta se repiten literalmente en la sentencia que ahora analizamos, lo que, de su lectura, lleva a pensar ya desde el principio que el TJUE mantendrá su doctrina. Aun así, lo interesante en este caso es conocer cómo ha resuelto las diferencias que presenta la ley alemana sobre la injerencia en los derechos de los ciudadanos alemanes, además de los nuevos argumentos presentados [que hemos relacionado antes].

Sirva como nota inicial que el propio Tribunal alemán reconoce (y así se refleja en la sentencia), en el apartado 34[461], que *"la exclusión de determinados medios de*

[459] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 37.

[460] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 38.

[461] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 34.

comunicación o de determinadas categorías de datos y la limitación del período de conservación no bastan para eliminar el riesgo de que se pueda dibujar un perfil completo de las personas afectadas, este riesgo se reduce cuando menos considerablemente en el marco de la aplicación de la normativa nacional en los litigios principales". Es decir, siendo conscientes de esa premisa, la argumentación alemana aporta otros elementos para justificar la segunda parte de la aseveración que hemos recogido.

Otra precisión, en este caso del TJUE, también hecha respecto del *Caso Commissioner of An Garda Síochána* es la constatación de que la Directiva 2002/58/CE regula no solo el acceso a los datos a través de garantías que eviten o prevengan los abusos, sino también, de forma particular, el principio de prohibición de su almacenamiento por terceros (apartado 39 de la sentencia mencionada y 56 de la sentencia que venimos analizando)[462]. Por último, también observa el Tribunal de Luxemburgo, como lo hizo ya anteriormente, que la conservación de datos de tráfico con el fin de hacerlos accesibles a las autoridades nacionales competentes suscita dudas sobre la injerencia en el derecho a la libertad de expresión recogido en el artículo 11 de la Carta. Por otro lado, este derecho, como tampoco los otros sobre los que sí se viene pronunciando recurrentemente (7 y 8 de la Carta), no constituyen prerrogativas absolutas, sino que deben ser puestos en contexto con la función que ejercen en la sociedad, lo que *"obliga a conciliar los distintos intereses legítimos en juego y establecer un marco jurídico que permita esta conciliación"* (apartado 65)[463]. Vuelve el Tribunal a reiterar su pronunciamiento de la sentencia de 5 de abril de 2022 respecto del requisito de proporcionalidad que una normativa nacional debe cumplir y respecto de la jerarquía entre los objetivos de interés general que permitan justificar una medida adoptada en virtud del artículo 15, apartado 1 de la Directiva de 2002.

A continuación, resuelve el Tribunal europeo cada una de las cuestiones prejudiciales que hemos resumido anteriormente:

[462] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 56.

[463] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 65.

- Sobre el alcance de los datos conservados, aunque se excluyen determinadas categorías, considera que los conservados siguen pudiendo permitir extraer conclusiones muy precisas sobre la vida privada de las personas afectadas, *"como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades ejercidas, sus relaciones sociales y los círculos que frecuentan y, en particular, facilitar los medios para determinar el perfil de esas personas"* (apartado 78)[464]. Según una de las empresas litigantes (SpaceNet), la exclusión de los datos relativos al correo electrónico solo representa una ínfima parte de los datos que se tratan por lo que, según el Abogado General de la Unión Europea (conclusión 60), la obligación de conservación prevista en la norma alemana se extiende a un *"amplísimo conjunto"* de datos de tráfico y de localización. Respecto de otra categoría de datos también excluida (los datos en los que se basan las comunicaciones de carácter social o religioso), el propio gobierno alemán reconoce que representa una parte reducida del conjunto de usuarios de telecomunicaciones en Alemania cuyos datos están sujetos a la obligación de conservación prevista por la normativa nacional controvertida en los litigios principales (sí se conservan los datos de los usuarios sujetos al secreto profesional, como los abogados y los periodistas).

  Por tanto, concluye el Tribunal que la conservación de los datos de tráfico y de localización prevista por la norma afecta a *"casi todas las personas que componen la población, sin que se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales"* (apartado 83) y no a una conservación selectiva como sostiene Alemania.

- Respecto del período de conservación, reconoce el Tribunal que son *"sensiblemente"* más cortos que los previstos en otras normativas nacionales, así como que es este un factor pertinente para tener en cuenta. Sin embargo, a renglón seguido (apartados 87 y 88)[465], a nuestro entender, le resta toda la importancia, pues declara que *"la gravedad de la injerencia se deriva del riesgo*

[464] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 83.

[465] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartados 87 y 88.

[…] de que estos [los datos conservados, considerados en su conjunto] permitan extraer conclusiones muy precisas sobre la vida privada de la persona o personas cuyos datos se han conservado y, en concreto, proporcionen los medios para establecer el perfil […]" y concluye que *"la conservación de los datos de tráfico o de localización […] es, en todo caso, grave, con independencia de la duración del período de conservación, de la cantidad y de la naturaleza de los datos conservados, cuando ese conjunto de datos pueda permitir extraer conclusiones muy precisas sobre la vida privada de la persona o personas afectadas"*[466]. En el caso concreto sobre el que se pronuncia, considera que una conservación durante diez semanas y cuatro semanas pueden permitir extraer conclusiones muy precisas sobre las personas. Con este argumento, nos surge la pregunta de por qué se ha cuestionado la disparidad de períodos de conservación que cada Estado miembro estableció a la hora de trasponer la Directiva de 2006 y se criticó el amplio margen temporal fijado (entre seis meses y dos años), si periodos tan cortos como los previstos en la norma alemana [a todas luces insuficientes para un gran número de investigaciones penales] son excesivos a los ojos del Tribunal. Incluso, si se reducen aún más, la conclusión, según los argumentos de este, debería ser la misma, vaciando así de contenido esa salvaguardia. Por tanto, entendemos que aquí se produce una novedad importante respecto de las sentencias anteriores y podemos concluir que la instancia europea proscribe la conservación de datos de forma generalizada e indiferenciada para cualquier periodo de conservación (salvo en amenazas a la seguridad nacional o para los datos de abonado/suscripción, siendo necesario aun así fijar plazos concretos, revisables) Para estos casos, el Tribunal no se ha pronunciado sobre qué considera un periodo de conservación adecuado y proporcionado.

- Sobre las medidas para proteger la información conservada de los riesgos de abuso y de acceso ilícito, considera el Tribunal que una normativa nacional que cumpla con los requisitos de la Directiva 2002/58/CE en materia de acceso a los datos conservados *"no puede, por naturaleza, ni limitar ni menos aún subsanar la injerencia grave originada por la conservación generalizada de tales datos*

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

con arreglo a esa normativa nacional" (apartado 91)[467]. No alcanzamos a comprender en toda su extensión la posición del TJUE en este apartado, al menos en cuanto a su aplicación práctica. En su primea sentencia cuestionó que la Directiva no preveía medidas claras y concretas para garantizar la seguridad de los datos, pero dado que una Directiva establece un marco mínimo sobre el que los Estados miembros pueden establecer mayores exigencias, en este caso, no permite que se puedan fijar medidas de seguridad más estrictas a nivel nacional y, de esa forma, reducir la gravedad de la injerencia en los derechos fundamentales, al menos en ese aspecto concreto.

- En este caso, como ya hizo también en el que resultó en la *Sentencia Commissioner of An Garda Síochána*, la Comisión Europea volvió a defender que la delincuencia particularmente grave podría asimilarse a una amenaza real para la seguridad nacional. El Tribunal mantiene su criterio negativo al respecto, que ya expusimos. No hay ningún matiz nuevo en esta ocasión.

- Vuelve el Tribunal a ilustrar mediante ejemplos concretos determinados supuestos en los que considera que se cumpliría su doctrina a la hora de establecer una conservación selectiva en base a criterios geográficos o grupos de personas, y exige que se evalúe de forma periódica el mantenimiento o evolución de los hechos y circunstancias que justificaron su adopción. De forma literal, pide, respecto de la selección de una zona o un grupo concreto: *"reaccionar al compás de los progresos en la lucha contra la delincuencia grave"* (apartado 111)[468]. Eso sí, recuerda una vez más (como ya hizo en la sentencia de 5 de abril) que *"incumbe a estos últimos [los Estados miembros] y no al Tribunal de Justicia identificar tales criterios [algún criterio distintivo que no sea ni personal ni geográfico para efectuar una conservación selectiva], partiendo de la base de que no puede tratarse de reinstaurar de esta manera una conservación generalizada e indiferenciada"* (apartado 112)[469]. Hasta el momento no nos consta que los Estados miembros hayan fijado ningún otro

[467] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 91.
[468] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 111.
[469] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 112.

criterio; más bien están centrados en buscar la forma de conseguir que la conservación sea, en la medida de lo posible, generalizada e indiferenciada. En este punto, después de varias sentencias que afianzan la doctrina del TJUE, creemos que no hay opciones para volver a la situación anterior y, por tanto, debería debatirse extraer el máximo rendimiento de esta nueva realidad, por ejemplo, siguiendo la vía que introduce aquí la instancia europea: buscar otros criterios válidos para el nuevo marco de un futuro régimen de conservación de datos a nivel de la Unión Europea. Tal vez haya otras opciones que aún no hemos identificado adecuadamente, pero que trataremos más adelante, como opción de futuro ya cada vez más cercano.

- Una vez más, sobre la capacidad de los Estados miembros para adoptar medidas en materia penal, reitera el Tribunal lo expresado ya en la *Sentencia Quadrature du Net y otros*, respecto de que *"ni siquiera las obligaciones positivas de los Estados miembros que pueden resultar, según el caso, de los artículos 3, 4 y 7 de la Carta y que se refieren […] a la adopción de normas que permitan combatir eficazmente los delitos pueden tener por efecto justificar injerencias tan graves como las que supone una normativa que establece una conservación de los datos de tráfico y de localización, en los derechos consagrados en los artículos 7 y 8 de la Carta de prácticamente toda la población sin que los datos de las personas afectadas puedan guardar una relación, al menos indirecta, con el objetivo perseguido"* (apartado 124). En definitiva, considera que son medidas desproporcionadas respecto del objetivo perseguido.

- Por último, acepta el Tribunal que las sentencias del TEDH invocadas por el Tribunal alemán[470] para sostener que el CEDH no se opone a normativas nacionales que establezcan una conservación generalizada e indiferenciada de los datos de tráfico y de localización, *"no pueden poner en entredicho la interpretación del artículo 15, apartado 1, de la Directiva 2002/58/CE que se deriva de las consideraciones anteriores"*. Reconoce que las sentencias del TEDH citadas se referían a interceptaciones de volúmenes de datos sobre

[470] Sentencia TEDH, de 25 de mayo de 2021, Big Brother Watch y otros c. Reino Unido (CE:ECHR:2021:0525JUD 005817013), y de 25 de mayo de 2021, Centrum för Rättvisa c. Suecia (CE:ECHR:2021:0525JUD 003535208).

comunicaciones internacionales, pero aun no discrepando con el Tribunal alemán en esa cuestión, recuerda el TJUE que el artículo 52, apartado 3 de la Carta tiene por objeto garantizar la coherencia necesaria entre los derechos que esta contiene y los que recoge el CEDH, *"sin perjuicio de la autonomía del Derecho de la Unión y del Tribunal de Justicia de la Unión Europea, de modo que solo deben tenerse en cuenta los correspondientes derechos del CEDH en vista de la interpretación de la Carta, como umbral de protección mínima"*[471] (apartado 125)[472]. El Tribunal europeo quiere hacer gala de su labor, ganada a lo largo de los años, de garante de los derechos de los europeos y, como hemos citado en capítulos anteriores, su papel de verdadero Tribunal Constitucional europeo, mostrando independencia y madurez respecto del Tribunal Europeo de Derechos Humanos. Tomás Mallén (2014; 240)[473] advierte precisamente de esas divergencias entre el TEDH y el TJUE y propone soluciones para evitarlas o minimizarlas: *"la optimización de la privacidad y de la seguridad debe venir de la mano de la articulación y sinergia entre los cánones europeos analizados, del Consejo de Europa y de la UE, para evitar que los posibles contenciosos paralelos se tornen en conflictos o episodios de divergencia, especialmente entre el TEDH y el TJUE, peligro que se ha intentado conjurar mediante la adhesión de la UE al CEDH ya impuesta por el Trabajo de Lisboa…".* Aun así, creemos constatar que siguen estando presentes en alguna medida.

Habida cuenta de que, como era previsible a la vista de la jurisprudencia previa y reiterada, se ha pronunciado en los mismos términos anteriores, el interés de esta sentencia, como hemos visto, está en el análisis que hace sobre determinados supuestos que ya introdujo en la Sentencia anterior del *Caso Commissioner of An Garda Síochána* y que ahora precisa más, para permitir, de forma limitada, la conservación de determinados datos de tráfico y de localización, así como de las direcciones IP de origen y de datos de identidad civil. Es llamativo que se refiere el Tribunal de forma constante a los datos de tráfico y de localización, considerando a los correspondientes a las

[471] Cita el TJUE la Sentencia de 17 de diciembre de 2020, Centraal Israëlitisch Consistorie van België y otros, C-336/19, EU:C:2020:1031, apartado 56)

[472] Sentencia TJUE *Casos SpaceNet AG y Telekom Deutschland GmbH*, C-793/19 y C-794/19, de 22 de septiembre de 2022, apartado 105.

[473] TOMÁS MALLÉN, B., *"Privacidad versus seguridad en el ámbito…",* op. cit., 240.

direcciones IP de origen y de usuario o identidad civil como incluidos en estas categorías, aunque no lo sean.

Nos llama también la atención la insistencia de la Comisión para vincular, en aras a justificar un aprovechamiento de los datos conservados de manera generalizada e indiferenciada que el Tribunal permite a efectos de la seguridad nacional, para investigaciones y actuaciones de lucha contra la delincuencia; como también llama la atención la contundente respuesta de rechazo a ese argumento por parte del Tribunal.

Lo más positivo de este nuevo pronunciamiento es que quizás pueda cambiar el rumbo de los trabajos que se están llevando a cabo en el seno del Consejo de la Unión Europea (junto con la Comisión), puesto que, al menos a nuestro entender, no queda más remedio que afrontar la situación desde la óptica de buscar otros criterios válidos para justificar la conservación selectiva, que será la que más frecuentemente se requiera en el marco de la lucha contra la delincuencia grave, y dejar de *retorcer* las sentencias para tratar de cambiar el criterio del Alto Tribunal. Quizás sirva también de acicate esta situación para explorar otras formas de avanzar, como podría ser a través del reglamento que está en fase de discusión entre los colegisladores, para actualizar la normativa sobre la privacidad de las comunicaciones. Continuar presentando cuestiones prejudiciales, muy probablemente no satisfaga plenamente a ninguna de las partes y, como observamos en las dos últimas sentencias, se pueda *cerrar alguna otra puerta que antes estaba entreabierta.*

CAPÍTULO VII. PNR E INTEROPERABILIDAD DE BASES DE DATOS EUROPEAS. OTROS EJEMPLOS DE LOS QUE EXTRAER CONCLUSIONES

En 2017, tras un intenso debate en el seno del Consejo de la Unión Europea y de la Comisión, y motivado por la sucesión de acontecimientos tanto de seguridad [como ataques terroristas en suelo europeo] como migratorios [aumento de la presión migratoria por la situación geopolítica de Siria, se asume que los ciudadanos exigen de sus instituciones, en este caso las comunitarias, que ejerzan más y mejores controles en las fronteras exteriores y en el espacio de Schengen. Una vez más, la Comisión, pero también el Consejo, consideran que estas medidas deben ser tomadas a nivel europeo, como única forma de alcanzar una gestión eficiente de la migración y aumentar también la seguridad interior.

La Unión Europea contaba ya en ese momento con herramientas para hacer frente a esta situación, entre otras, se habían puesto en funcionamiento determinadas bases de datos y sistemas europeos concebidos para la gestión de las fronteras, la migración y la seguridad. Se hablaba también ya en ese momento de la necesidad de acelerar el proceso de puesta en funcionamiento de otras bases nuevas sobre las que se estaba trabajando, pidiendo los representantes políticos avanzar para alcanzar consenso sobre los borradores de textos normativos que la Comisión había presentado a los Estados miembros (para su discusión en el Consejo y en el Parlamento Europeo, como colegislador en el procedimiento ordinario que se sigue en este tipo de expedientes). Ahora, se trataba de acelerar el ritmo con las bases de nueva creación y de poner sobre la mesa una nueva propuesta que permitiera conseguir algo con lo que los servicios policiales y agentes de frontera habían soñado siempre, tanto en sus respectivos ámbitos nacionales como para el proceso de integración europea.

Siempre que se trata de bases de datos y sistemas de gestión de información, y del acceso y tratamiento de los datos personales que estas contienen, surge el debate necesario y obligatorio respecto del respeto de los derechos fundamentales de los ciudadanos, especialmente del derecho a la privacidad y a la protección de los datos

personales y de su relación con la Seguridad; en este caso a través de la gestión eficiente de las fronteras exteriores de la Unión[474].

1. Interoperabilidad de determinadas bases de datos europeas

El proyecto[475] de interoperabilidad comenzó en 2016[476] con un estudio previo en el que participaron numerosos actores, a través de un grupo de trabajo que identificó una serie de deficiencias estructurales en la arquitectura de gestión de la información de la Unión Europea y que quedaron reflejadas en un documento de conclusiones. El Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad abordó los aspectos jurídicos, técnicos y operativos de la mejora de la interoperabilidad de los sistemas centrales de la UE para la gestión de las fronteras y la Seguridad, así como su necesidad y proporcionalidad e incidencia en el derecho a la protección de los datos personales. En 2017 se publicó el informe final[477] de conclusiones del grupo de trabajo y se aportaron recomendaciones. La principal conclusión a la que se llegó fue el apoyo a la viabilidad del proyecto desde el punto de vista técnico y la necesidad y proporcionalidad de las medidas propuestas, de forma que se podrían alcanzar ventajas operativas sin producir una injerencia desproporcionada de conformidad con los requisitos de protección de datos.

Las reacciones a este informe por parte de otras instituciones y organismos europeos relevantes fueron favorables. Así, tanto la Agencia Europea de los Derechos

[474] El debate en el seno de las instituciones europeas respecto de la relación entre migración y Seguridad es también complejo y controvertido, por cuanto unos Estados miembros creen que no se puede asociar migración con inseguridad y otros que, sin vincular directamente una y otra cosa, sí creen que hay influencia o aprovechamiento del fenómeno migratorio para que delincuentes y terroristas puedan cruzar las fronteras y presentar un riesgo o amenaza a la seguridad de los europeos. No es objeto de este trabajo analizar esa polémica, ya que tanto si existe relación como si no, hay consenso respecto de que se han de respetar igualmente los derechos fundamentales de las personas cuyos datos se recogen y conservan en las bases de datos europeas -y nacionales- y en los sistemas que permitan hacer interoperables unos y otros.

[475] Podríamos denominarlo como *"macroproyecto"*, por la envergadura de las bases a las que afecta, por la inversión que será necesaria para hacerlo realidad y porque supondrá un salto cualitativo muy importante en la gestión de la información en la UE.

[476] Por tanto, cuando el TJUE ya había dictado la primera de las sentencias respecto de la Directiva de Conservación de Datos y la había declarado nula. Ese mismo año se pronunció de nuevo, en el mes de diciembre confirmando su doctrina anterior.

[477] Disponible en http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

Fundamentales (FRA)[478], como el Supervisor Europeo de Protección de Datos participaron de forma activa en las reuniones del grupo de alto nivel y apoyaron su contenido. El Parlamento Europeo, aunque asistió como observador, a través de representantes de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, también dio su visto bueno a las conclusiones del grupo de trabajo. En definitiva, aunque en este momento todavía no se habían presentado las propuestas normativas para materializar lo analizado por los expertos, no parecía haber reticencias respecto del impacto desproporcionado en los derechos fundamentales de las soluciones que se pretendían adoptar para mejorar la gestión de los flujos migratorios y la seguridad interior de la Unión; como sí había ocurrido desde el principio con la iniciativa para establecer un sistema de conservación de datos de comunicaciones electrónicas por los proveedores de este tipo de servicios en la UE.

Posteriormente, la Comisión hizo suyas las propuestas de los expertos y las incorporó a su séptimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva, en lo que consideró *"un nuevo enfoque para la gestión de los datos de las fronteras, la seguridad y la migración en el que todos los sistemas centralizados de información de la UE para la gestión de la seguridad, las fronteras y la migración sean interoperables, con pleno respeto de los derechos fundamentales"*[479] (COM, 2017; 3).

El Consejo de la Unión Europea también avaló la propuesta, a través de los ministros de Justicia e Interior, en su reunión de junio de 2017, y el Consejo Europeo hizo lo mismo en su reunión de jefes de Estado y de Gobierno del mismo mes, de forma que se instaba a la Comisión a presentar lo antes posible un proyecto legislativo que permitiera llevar a la práctica las recomendaciones del grupo de alto nivel. Aún no hemos mencionado las bases concretas a las que afectaría la propuesta normativa, pero por la naturaleza de los objetivos que pretende alcanzar la interoperabilidad de estas,

[478] La Agencia europea de los Derechos Fundamentales (FRA, por sus siglas en inglés) proporciona a los responsables de la toma de decisiones nacionales y de la UE asesoramiento independiente, contribuyendo así a que la creación de debates, políticas y legislación en materia de derechos fundamentales sea mejor informada y más específica. Para profundizar, vid. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/fra_es

[479] COM (2017) 261 final en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0261&from=EN .

podemos pensar que afectarán al trabajo de los servicios policiales. De hecho, ya había apuntado el grupo de expertos que se pretendía conseguir racionalizar en mayor medida las necesidades operativas, así como darles más coherencia y eficacia.

Las bases de datos y sistemas de gestión de la información involucradas en la propuesta eran[480]:

- El *Sistema de Información de Schengen (SIS)*, que recoge una amplia variedad de datos relativos a personas y objetos y que permite, en base a estos, denegaciones de entrada o de estancia en la UE, establecer órdenes de detención europea, grabar personas desparecidas o establecer procedimientos de asistencia judicial o de vigilancia sobre personas u objetos, además de identificar documentos robados, perdidos o invalidados[481].
- El sistema *Eurodac*, que contiene datos dactiloscópicos de los solicitantes de asilo y de nacionales de terceros países que han cruzado las fronteras exteriores de forma irregular o que se encuentran en situación ilegal en un Estado miembro.
- El *Sistema de Información de Visados (VIS)*, que contiene datos sobre los visados para estancias de corta duración[482].

[480] Según recogen la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (fronteras y visados) y por el que se modifican la Decisión 2004/512/CE del Consejo, el Reglamento (CE) nº. 767/2008, la Decisión 2008/633/JAI del Consejo, el Reglamento (UE) 2016/399 y el Reglamento (UE) 2017/2226, en http://delegates.consilium.europa.eu/index.html?targetPath=private/controller/documents:documentSaveAs&docType=ST&docNumber=15119&docQualifier=INIT&docYear=2017&language=ES&docFormat=PDF y la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (cooperación policial y judicial, asilo y migración), COM (2017) 784 final, en https://delegates.consilium,europa.eu/index.html?targetPath=private/controller/documents:documentSaveAs&docType=ST&docNumber=15729docQualifier=INIT&docYear=2017&language=ES&docFormat=PDF

[481] De hecho, es la única base realmente policial de las que se incluyeron en el proyecto de interoperabilidad. El resto, tanto las existentes, que se reflejan a continuación, como las que estaban en ese momento en fase de creación de sus instrumentos legislativos propios, afectaban al trabajo de los agentes de fronteras, que en muchos Estados miembros no tiene por qué ser desempeñados por cuerpos policiales, o no por todos los cuerpos policiales existentes en el país. En ese momento, se estaba trabajando sobre tres propuestas legislativas que ampliaban este sistema, para adaptarlo a las nuevas realidades de seguridad de la Unión.

[482] En ese momento, este sistema estaba en fase de revisión y modificación de su reglamento, para adaptarlo a la nueva realidad, ampliar su mandato y permitir también su integración en las soluciones de interoperabilidad que se pretendía implementar.

Además de los anteriores, los colegisladores estaban trabajando ya sobre la creación de otros tres sistemas, en base a las propuestas que la Comisión presentó en 2016 y 2017:

- El *Sistema de Entradas y Salidas (SES)*, que permitiría sustituir el sellado manual de los pasaportes, registrando electrónicamente el nombre, el tipo de documento de viaje, los datos biométricos y la fecha y lugar de entrada y salida de los nacionales de terceros países que visiten el espacio Schengen para estancias de corta duración[483].
- El *Sistema Europeo de Información y Autorización de Viajes (SEIAV)*[484], que recopilará y verificará de forma automatizada la información presentada por los nacionales de terceros países exentos de la obligación de visado antes de su viaje al espacio Schengen.
- El *Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN)*, que permitirá el intercambio electrónico de información sobre las condenas dictadas contra nacionales de terceros países por los tribunales penales de la Unión Europea[485].

Otros sistemas de información europeos de gestión descentralizada o los puramente nacionales quedaron fuera de la propuesta. Sin embargo, nos referiremos más adelante a uno que nos interesa de forma particular, por su relación directa con la Directiva de Conservación de Datos respecto de la injerencia en los derechos de los ciudadanos.

Las soluciones que a nivel europeo incluía la interoperabilidad se mencionan a continuación, sin entrar en detalles muy técnicos, para no desviarnos del propósito de este capítulo: el análisis de en qué medida son acciones necesarias y proporcionadas

[483] Este sistema está aprobado y en vigor, pero todavía se encuentra en fase de ejecución por los Estados miembros, supervisados por la Comisión. Debería estar en funcionamiento pleno en 2023, aunque la pandemia del COVID-19 ha producido retrasos.

[484] Este sistema está aprobado y en vigor, pero todavía se encuentra en fase de ejecución por los Estados miembros, supervisados por la Comisión. Debería estar en funcionamiento pleno en 2023, aunque la pandemia del COVID-19 ha producido retrasos.

[485] Este sistema está aprobado y en vigor, pero todavía se encuentra en fase de ejecución por los Estados miembros, supervisados por la Comisión. Debería estar en funcionamiento pleno en 2023, aunque la pandemia del COVID-19 ha producido retrasos.

para alcanzar el fin perseguido y qué similitudes o diferencias pueden tener respecto de las que se tomaron en la Directiva 2006/24/CE:

- *Portal Europeo de Búsqueda (PEB)*. Es el componente que permitirá la búsqueda simultánea en múltiples sistemas (SIS, Eurodac, VIS, SES, SEIAV y ECRIS-TCN) utilizando datos de identidad (biométricos y biográficos) y permitirá a los usuarios un acceso rápido, ininterrumpido, eficiente, sistemático y controlado a la información contenida en estos sistemas. Es lo que se denomina *ventanilla única*. A través de una única introducción de datos, se consulta a todos los sistemas y se ofrece una respuesta respecto de si hay coincidencias con esos datos en alguno/s de ellos. La Comisión considera en su propuesta que el portal no almacena nuevos datos ni realiza tratamiento de nuevos datos y, en consecuencia, respeta las normas de protección de datos y de control del acceso a los sistemas subyacentes[486].

- *Servicio de correspondencia biométrica compartido (SCB compartido)*. Este componente permite la consulta y comparación de datos biométricos (impresiones dactilares e imágenes faciales) de aquellos sistemas que almacenan este tipo de información[487]. Los datos biométricos se conservarán exclusivamente en los sistemas subyacentes, por lo que en el SCB compartido solo se crearía una plantilla[488] de las muestras biométricas almacenadas en las bases y sistemas. Lo que se pretende es detectar conexiones entre datos biométricos e identidades asumidas por una persona en los distintos sistemas centrales.

- *Registro común de datos de identidad (RCDI)*. Este componente almacenará los datos de identidad biográficos[489] y biométricos de los nacionales de terceros países registrados en Eurodac, el VIS, el SES, el SEIAV y ECRIS-TCN. Cada uno de estos sistemas registra o registrará los datos biométricos de personas concretas por motivos específicos y así seguirá siendo. El RCDI almacenará determinados datos de identidad, pero seguirán *perteneciendo* a los respectivos sistemas subyacentes.

[486] Los sistemas en los que realiza la consulta.
[487] El SIS, el VIS, el SES y el ECRIS-TCN.
[488] Una representación matemática de las muestras biométricas.
[489] Los datos biográficos que figuran en el documento de viaje incluyen: apellidos, nombre, sexo, fecha de nacimiento y número de documento de viaje. No se incluyen direcciones, nombres anteriores, datos biométricos, etcétera.

- *Detector de identidades múltiples (DIM)*. Verificará si los datos de identidad consultados existen en más de uno de los sistemas conectados y, para ello, cubrirá los sistemas que almacenan o almacenarán datos de identidad en el RCDI, así como el SIS[490], permitiendo la detección de identidades múltiples vinculadas con el mismo conjunto de datos biométricos, con la doble finalidad de garantizar la identificación correcta de las personas *de buena fe*[491] y de luchar contra la usurpación de identidad[492].

Es necesario señalar cómo resuelve la propuesta el acceso a los datos que recogen cada una de las bases y sistemas, por aquellos que no están habilitados en un principio según los reglamentos particulares de creación de cada uno de los sistemas. Como hemos mencionado antes, excepto el SIS, las cinco bases y sistemas que se harán interoperables habilitan (de acuerdo con los procedimientos y requisitos que cada norma establece) el acceso a los datos a los *agentes de fronteras* y, como también destacábamos, no tienen por qué corresponderse siempre y en todos los países con cuerpos policiales. En cambio, ahora se prevé que los cuerpos policiales, los responsables de la garantizar la seguridad de los ciudadanos, puedan tener acceso a esos datos en cumplimiento de sus funciones y en circunstancias legalmente previstas ¡Hagamos aquí un inciso¡ Ciertamente, no es una situación plenamente equivalente a la que se producía respecto de la Directiva 2006/24/CE, en cuanto a la interacción de actores alrededor de la conservación y el acceso a los datos, ni tampoco respecto de las finalidades previstas; pero sí nos parece que existe alguna analogía. De forma más detallada, estas bases se han creado para conservar datos a los que tendrán acceso los agentes de frontera y ahora se establecerá un sistema que permitirá de forma ágil y rápida que los servicios policiales también dispongan de esos datos (siguiendo los requisitos que ya se preveían en los reglamentos individuales de cada base de dato, puesto que no se modifican las condiciones de acceso). En la Directiva de conservación

[490] La compleja arquitectura técnica del SIS, que contiene copias nacionales de determinados Estados miembros, además de copias parciales y posibles sistemas nacionales de correspondencia de datos biométricos, haría que el RCDI fuera muy complejo o incluso económicamente inviable, por lo que se dejó fuera.

[491] Personas sobre las que aparece una supuesta doble identidad en diferentes bases de datos, pero que es debido a causas ajenas a su actuación maliciosa o intencionada; sino por errores de agentes externos a los afectados.

[492] El DIM permitirá establecer que diferentes nombres corresponden a la misma identidad y permitirá resolver la usurpación de identidad, que constituye una grave violación de la seguridad.

de datos se disponía que los datos conservados para los fines comerciales y de negocio de los operadores de telecomunicaciones [al menos esos] pudieran ponerse a disposición también de los servicios policiales en determinados supuestos y cumpliendo con un determinado procedimiento establecido.

La consulta policial constituye un objetivo accesorio o secundario a Eurodac, al VIS, al SES y al SEIAV. En consecuencia, la posibilidad de acceder a los datos almacenados en esos sistemas a efectos policiales es limitada. Hasta ahora, la consulta a estas bases de datos *no policiales* se viene haciendo con fines de prevención, investigación, detección o enjuiciamiento de actos de terrorismo y otros delitos graves[493] y, como apuntábamos en el párrafo anterior, siguiendo el procedimiento previsto para cada una de esas bases de datos: no se pueden consultar directamente sino que se deben seguir diferentes condiciones de acceso y cumplir con salvaguardias específicas, lo que en muchos casos, por lentitud de los procedimientos administrativos [en muchas ocasiones no se puede demorar la obtención de la información cuando la persona sobre la que se realiza la consulta está presente, lo que hace inoperativa la solicitud y, en no pocas ocasiones, podría perderse una información crucial que afecta a la seguridad de los ciudadanos] y porque los accesos han de solicitarse a los responsables de cada una de las bases de forma independiente, lo que hace que no siempre se recurra a estas fuentes de información y puedan generarse no solo situaciones que pongan en riesgo la seguridad, (como decíamos antes) sino también la pérdida de oportunidades para esclarecer determinados delitos graves. También puede ocurrir que cuando se recibe la contestación ya no sea una información oportuna, con los mismos efectos negativos sobre la seguridad de los ciudadanos.

Para hacer frente a esta situación y así ganar en eficacia, sin obviar los requisitos legales que se establecen en cada una de las normas particulares de creación de las bases y sistemas afectados, la propuesta de la Comisión consistía en un planteamiento en dos etapas del acceso de los cuerpos policiales:

[493] Mismos fines que los previstos para el acceso a los datos conservados de acuerdo con la Directiva 2006/24/CE y las leyes de trasposición a nivel de los Estados miembros.

- en la primera, el policía realizaría una consulta sobre una determinada persona, utilizando los datos de identidad, el documento de viaje o los datos biométricos de esa persona, para comprobar si en alguna de las bases o sistemas existe información sobre la persona (u objeto) buscada. Si la hay, se recibirá una respuesta indicando qué sistema o sistemas contienen datos al respecto, pero no tendrá acceso a la información concreta de los sistemas subyacentes afectados.

- en la segunda etapa, el agente de policía podrá solicitar el acceso a cada uno de los sistemas que contiene los datos, según la respuesta recibida en la primera fase, y así disponer del expediente completo sobre esa persona, pero tendrá que seguir los procedimientos establecidos en la normativa de cada sistema, lo que suele requerir una autorización previa de una autoridad designada -como hasta ahora- y se registrarán los datos del solicitante.

Este nuevo planteamiento, aunque no fue aceptado plenamente por los representantes de los cuerpos policiales que acudían a las reuniones de los grupos de trabajo del Consejo de la Unión Europea para la negociación del expediente de interoperabilidad, ya que pretendían agilizar el procedimiento (al menos para casos de urgencia), consideramos que ahorra tiempo y gana en eficacia en las investigaciones, al cribar de una forma casi instantánea aquellas bases y sistemas que disponen de información, descartando las que no, por lo que el procedimiento para acceder al expediente completo se hará más rápido y sencillo.

1. Base jurídica, necesidad y proporcionalidad

El proyecto de interoperabilidad consta de dos reglamentos europeos[494], habiéndose optado por dos instrumentos legislativos en vez de uno debido a lo que en *Bruselas* se conoce como *geometría variable*, puesto que no todos los Estados miembros participan plenamente del acervo comunitario; o porque hay que integrar también a los países asociados a Schengen, para la parte en la que se ven concernidos por las medidas que en los reglamentos se recogen, etcétera. No obstante, las diferencias

[494] Uno de los reglamentos está referido a fronteras y visados y el otro a cooperación policial y judicial, migración y asilo.

entre ambos son menores y no tienen ninguna implicación digna de mención a los efectos de nuestra investigación, por lo que hacemos esta mención únicamente a modo de introducción aclaratoria.

En este caso, la base jurídica principal utilizada para la propuesta de fronteras y visados fue la que ofrecen los artículos 16.2, 74 y 77.2 del Tratado de Funcionamiento de la Unión Europea, que al contrario que la base jurídica utilizada para la propuesta de Directiva de Conservación de Datos, son artículos relativos al espacio de Libertad, Justicia y Seguridad y no de desarrollo del Mercado Interior. El artículo 74 habilita al Consejo a *"adoptar medidas relativas a la política de visados y otros permisos de residencia de corta duración, los controles de personas que crucen las fronteras exteriores, cualquier medida necesaria para el restablecimiento progresivo de un sistema integrado de gestión de fronteras exteriores y la ausencia de controles de las personas, con independencia de su nacionalidad, cuando crucen las fronteras interiores"* (TFUE, 2010; C 83/75). Para la propuesta de cooperación policial y judicial, asilo y migración se utilizaron los artículos 16.2, 74 y 78.2, 82.1, 85.1, 87.2 y 88.2 del TFUE. Precisamente, los artículos 88.1 y 87.2 facultan a la Unión a adoptar *"medidas de refuerzo de la cooperación policial y judicial en relación con la recogida, el almacenamiento, el tratamiento, el análisis y el intercambio de información pertinente"* (TFUE, 2010; C 83/84 y ss.).

Respecto del principio de proporcionalidad, en la evaluación de impacto que acompaña a la propuesta de reglamentos[495], la Comisión argumenta que *"las opciones políticas presentadas se consideran proporcionadas y no van más allá de lo necesario para alcanzar los objetivos acordados"*.

[495] Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending ……, en https://delegates.consilium.europa.eu/index.html?targetPath=private/controller/documents:documentSaveAs&docType=ST&docNumber=15119&docQualifier=ADD%202&docYear=2017&language=EN&docFormat=PDF

Respecto del instrumento elegido, se propone el reglamento en vez de la directiva. En este caso, todos los sistemas y bases de datos han sido creados o están en proceso de negociación mediante reglamentos y el funcionamiento interoperable de todos ellos se considera que debe serlo también mediante el mismo instrumento jurídico.

Otro aspecto relevante para tener en cuenta en estas propuestas es el relativo a la evaluación que la Comisión realiza respecto del impacto en los derechos fundamentales, en particular en el derecho a la protección de los datos personales. La Comisión considera que, de acuerdo con el artículo 51, apartado 1 de la Carta, *"las Instituciones de la Unión y los Estados miembros deben observar, cuando aplican el Derecho de la Unión, las oportunidades que brinda la interoperabilidad como medida para mejorar la seguridad y la protección de las fronteras exteriores, conciliándolas con la obligación de garantizar que las interferencias con los derechos fundamentales que pudieran derivarse del nuevo 'entorno de interoperabilidad' se limiten a lo estrictamente necesario para alcanzar realmente los objetivos de interés general perseguidos, respetando el principio de proporcionalidad que prevé el artículo 52, apartado 1 de la Carta"* (COM, 2017; 12) . En ese sentido, considera que las soluciones de interoperabilidad que propone son componentes complementarios de los sistemas existentes y, como tales, no alterarán el equilibrio ya garantizado por cada uno de esos sistemas individualmente considerados en cuanto a su impacto en los derechos fundamentales.

Resulta curioso que, respecto del impacto de esas soluciones de interoperabilidad en otros derechos fundamentales afectados, como son el respeto a la vida privada, considera la Comisión que efectivamente se producirá un impacto, pero positivo, puesto que se pueden evitar confusiones de identidad. Además, la realización de controles basados en datos biométricos cree la Comisión que *"puede percibirse como una interferencia con el derecho de la persona a la dignidad humana, en particular, si esos controles se perciben como humillantes"* (COM, 2017; 29). Sin

embargo, menciona una encuesta[496] realizada por la Agencia de los Derechos Fundamentales de la UE en la que *"se preguntó a los encuestados si creían que el conocimiento de sus datos biométricos en el contexto del control de fronteras podría resultar humillante y la mayoría de los encuestados consideró que no lo sería"* (COM, 2017; 14).

Otros argumentos de la propuesta que deben ser resaltados respecto de la afectación a derechos fundamentales por las soluciones de interoperabilidad son:

- Se justifica la bondad que supone la adopción de medidas preventivas hacia una mejor seguridad. Es muy interesante este argumento, por cuanto hemos visto que la conservación de datos que preveía la Directiva 2006/24/CE fue rechazada por el Tribunal europeo, entre otros argumentos, por el carácter preventivo a los efectos de la seguridad pública y nacional. Sin embargo, en este caso cree la Comisión que estas medidas pueden favorecer la defensa del derecho a la vida de las personas[497], lo que exige de las autoridades la adopción de medidas operativas de carácter preventivo para proteger a los ciudadanos ante situaciones de peligro a sus vidas, así como para mantener la efectividad de la prohibición de la esclavitud y del trabajo forzado [en casos relacionados con personas que huyen de sus países por motivos de persecución política o de otro tipo que afecte a su vida o a su integridad][498]. De ese modo, argumenta que, a través de una identificación más fiable y más accesible y sencilla, la interoperabilidad puede ayudar a detectar niños desaparecidos o niños sometidos a situaciones de trata y facilitar respuestas oportunas y precisas.
- Una identificación fidedigna, más asequible y sencilla también podría coadyuvar a que se respete realmente el derecho al asilo[499] y el principio de no devolución[500], de forma que la interoperabilidad podría evitar situaciones en las que los solicitantes de asilo sean tratados de una forma contraria a la ley. También, podría contribuir a

[496] Encuesta del FRA en el marco del proyecto piloto sobre fronteras inteligentes de eu-LISA - opiniones y experiencias de los viajeros sobre *"fronteras inteligentes"*, Informe de la Agencia de Derechos Fundamentales de la UE, en http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf

[497] Artículo 2 de la Carta.

[498] Artículo 5 de la Carta.

[499] Artículo 18 de la Carta.

[500] Artículo 19 de la Carta.

detectar situaciones de usurpación de identidad, reduciendo al mismo tiempo el intercambio de datos sobre esos mismos solicitantes de asilo con el objetivo de establecer la identidad de la persona y de obtener documentos de viaje, lo que podría arriesgar las vidas de determinadas personas, cuando la solicitud de hace a sus países de origen.

Respecto del derecho a la protección de datos, en el momento de presentación del marco de interoperabilidad ya estaba en vigor el denominado *"paquete de protección de datos de la Unión Europea"* que ha sustituido a la Directiva 95/46/CE de protección de datos y a la Decisión Marco 2008/977/JAI, por lo que el régimen de protección de datos en la Unión Europea se había actualizado y, según la opinión de una buena parte de los expertos, se había convertido en uno de los más exigentes del mundo respecto de la protección de los datos personales de los ciudadanos europeos. En el Reglamento general se establece que la libre circulación de datos no estará restringida por causa de la protección, pero cualquier limitación del ejercicio de los derechos fundamentales protegidos por la Carta deberá cumplir con los siguientes criterios recogidos en su artículo 52, apartado 1 . Considera la Comisión que las propuestas integran todos los criterios de la Carta que recoge el Reglamento general de protección de datos[501]:

> "se basa en los principios de protección de datos desde el diseño y por defecto; incluye todas las disposiciones apropiadas que limitan el tratamiento de datos a lo necesario para el propósito específico y conceden acceso a los datos únicamente a aquellas entidades que *'necesitan saber'*; los plazos de conservación son adecuados y limitados; el acceso a los datos está reservado exclusivamente al personal debidamente autorizado de las administraciones de los Estados miembros o de los organismos de la UE competentes para los fines específicos de cada sistema de información, y se limita a la medida en que los

[501] El artículo 52, apartado 1 de la Carta establece que, *"para ser legal, cualquier limitación del ejercicio de los derechos fundamentales protegidos por la Carta debe cumplir los siguientes criterios:*

- *Debe ser establecida por ley;*
- *Debe respetar el contenido esencial de los derechos;*
- *Debe responder efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás;*
- *Debe ser necesaria y*
- *Debe ser proporcional"*.

datos sean necesarios para el desempeño de las tareas conformes a dichos fines" (COM, 2017; 35).

El SEPD, en su informe sobre la propuesta de los reglamentos[502] analiza el contenido de los textos desde el punto de vista de la función que le encomienda el Reglamento europeo 45/2001[503] relativo a la protección de las personas físicas respecto del tratamiento de datos personales por las instituciones y organismos comunitarios, ahora sustituido por el Reglamento (UE) 2018/1725, de 23 de octubre de 2018[504] y concluye apoyando la interoperabilidad y su utilidad como herramienta para satisfacer las necesidades, que considera legítimas, de las autoridades competentes en el intercambio de información que contienen los sistemas de información a gran escala de la Unión Europea, *"siempre que se cumplan los requisitos básicos de necesidad y proporcionalidad"*[505]. No obstante, puesto que en las propuestas de reglamentos se deja abierta la posibilidad de extender las soluciones propuestas a otras bases o sistemas futuros, el SEPD avisa de que, en ese caso, habría que volver a analizar el cumplimiento de los criterios de necesidad y proporcionalidad y la injerencia de esas nuevas medidas en los derechos fundamentales; cuestión que parece del todo lógica. Aun así, entendemos que la Comisión tendría que instar un nuevo procedimiento legislativo, con todas las prevenciones y requisitos que se han seguido a la hora de presentar estas propuestas de reglamento. Por tanto, el *"aviso"* del Supervisor europeo no deja de ser más que la constancia por escrito de algo que, si se produce, será así y, entre los informes que se requerirán, sin duda alguna, estará también el de ese organismo, como ha ocurrido para los reglamentos actuales de interoperabilidad.

[502] European Data Protection Supervisor (EDPS), *"Reflection paper of the European DataProtection Supervisor on the interoperability of information systems in the area of Freedom, Security and Justice"*, 17 November 2017, en https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf

[503] Reglamento (CE) nº. 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, OJ L 8, 12.1.2001, p. 1-22, en http://data.europa.eu/eli/reg/2001/45/oj

[504] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismo de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº. 45/2001 y la Decisión nº. 1247/2002/CE, OJ L 295, 21.11.2018, p. 39-98, en http://data.europa.eu/eli/reg/2018/1725/oj

[505] European Data Protection Supervisor (EDPS), Reflection paper…, *op. cit*. p. 12

Recuerda también el Supervisor la importancia de justificar de forma preliminar la necesidad y la proporcionalidad del tratamiento, puesto que el cumplimiento de las normas de protección de datos trasciende el que s hayan sido tenidas en cuenta por defecto en el diseño; en este caso, en el diseño de los componentes de interoperabilidad que prevén los reglamentos. Finaliza el informe dejando la puerta abierta a un análisis posterior, a medida que se fuera avanzando en el expediente legislativo, quizás conocedor de que las propuestas iniciales suelen modificarse, en muchos casos de forma sustancial[506].

En mayo de 2019 se aprobaron los dos Reglamentos europeos[507] tras un largo proceso legislativo y político, y entraron en vigor en junio de ese mismo año. Una de las conclusiones más aceptadas por todos los actores intervinientes en este ámbito es que la interoperabilidad cambiará el modo en que los agentes encargados de la aplicación de la ley (servicios policiales y agentes de fronteras, fundamentalmente) de primera línea llevarán a cabo diversas tareas cotidianas: tramitar solicitudes de visado, realizar investigaciones penales, registrar a migrantes y efectuar controles fronterizos de primera línea, por mencionar tan solo algunas. Otro hecho importante es que la interoperabilidad tendrá también un efecto positivo en la cooperación entre las autoridades. No obstante, el verdadero efecto de la interoperabilidad dependerá de su ejecución técnica y en eso no solo estarán concernidos los servicios de la Comisión Europea, sino que obliga también a los Estados miembros, puesto que será preciso crear una estructura integral de coordinación que reúna a los usuarios operativos y a los expertos técnicos que desarrollan sistemas de tecnología de la información; y deberá contarse también con

[506] En el momento de emisión del informe, solo se conocían las propuestas de la Comisión y apenas se había empezado a analizar en el seno del Consejo de la UE. Hoy día, los reglamentos han sido aprobados y están en vigor, aunque no serán ejecutados hasta 2023, salvo previsibles prórrogas adicionales.

[507] Reglamento (UE) 2019/817 del Parlamento y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) nº. 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, OJ L 135, 22.5.2019, p-27-84, en http://data.europa.eu/eli/reg/2019/817/oj

Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816, OJ L 135, 22.5.2019, p. 85-135, en http://data.europa.eu/eli/reg/2019/818/oj

apoyo y orientación políticos, para que se establezca una coordinación nacional dotada de recursos humanos y financieros suficientes.

En este caso, a diferencia de las medidas que recogió la Directiva de Conservación de Datos, por la propia naturaleza de un reglamento, que difiere de lo que regula una directiva, y quizás también porque se aprende de experiencias fallidas anteriores, la Comisión ha optado por una estructura centralizada en algunas partes y con desarrollos técnicos y organizativos también a nivel nacional, pero con financiación y dirección desde Bruselas. En consecuencia, si se presentara alguna cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea que derivara en la declaración de nulidad de los reglamentos, la caída de todo el entramado sería automática tanto a nivel central como de los Estados miembros, no como ha ocurrido en el caso de la Directiva 2006/24/CE. En la fecha de redacción de esta tesis, no se tiene constancia de que se haya solicitado pronunciamiento alguno del Tribunal de Luxemburgo; máxime cuando, aunque los reglamentos están en vigor, no se ejecutarán hasta finales de 2023. Un indicador positivo es que, en esta ocasión, no ha habido oposición directa por ninguna de las instituciones ni organismos que, sin embargo, en el caso de la Directiva de Protección de Datos ya pronosticaron, con mucha antelación, el final de ese instrumento legislativo. Quizás la Comisión debería haber *escuchado aquellas voces* a tiempo y se hubiera podido reconducir la situación a tiempo. De cualquier modo, habrá que esperar a que comiencen a funcionar los desarrollos de la interoperabilidad.

Mientras tanto, y a falta de conocer la fecha de puesta en funcionamiento y los desarrollos finales que lo hagan posible, los expertos consideran que la interoperabilidad quebrará los comportamientos operativos y técnicos que surgen cuando se desarrollan distintos procesos de trabajo y sistemas de tecnología de la información. El método de recogida de datos, la calidad de los datos recogidos y la determinación de los datos que deben registrarse son cuestiones que afectarán al modo en que estos podrán ser utilizados por otros procesos y a la magnitud de las ventajas que se podrán obtener del marco de interoperabilidad. Como adelantaba ya en 2017 el Supervisor Europeo de Protección de Datos, los expertos opinan también que la

interoperabilidad creará una interconexión entre los diferentes reglamentos de la Unión Europea y propuestas relacionadas con ellos; es decir, posibles modificaciones sobre los reglamentos particulares de las bases de datos y sistemas subyacentes (u otros que se puedan crear en el futuro) y eso exigirá tenerlos presentes de cara a nuevas propuestas legislativas y al consiguiente análisis de la injerencia en los derechos fundamentales y la necesidad y proporcionalidad de las medidas que se adopten.

2. El registro de nombres de los pasajeros de líneas aéreas (PNR) al servicio de la seguridad de los europeos

En los últimos años, un número cada vez mayor de países -no sólo los Estados miembros de la UE- y organizaciones internacionales han reconocido el valor de la utilización de los datos PNR *(acrónimo de Passenger Name Record)* [508] como instrumento policial. El establecimiento de un mecanismo PNR y la aplicación de la Directiva PNR deben considerarse en el contexto de esta tendencia internacional más amplia.

También fueron los atentados terroristas que tuvieron lugar en los Estados Unidos en 2001, en Madrid en 2004 y en Londres en 2005 los que dieron lugar a la adopción de, entre otras medidas, los instrumentos legislativos sobre la recogida y el intercambio de datos PNR. Para establecer los elementos de la política exterior de la UE en materia de PNR, la Comisión presentó en 2003 una primera Comunicación *"Sobre el enfoque global de las transferencias de datos del registro de nombres de los pasajeros (PNR) a terceros países"*[509], que fue revisada en una Comunicación adoptada en 2010[510].

Estos criterios generales constituyeron la base de las renegociaciones de los acuerdos PNR con EE. UU., Australia y Canadá, que condujeron a la celebración de

[508] Se utiliza el acrónimo inglés, aunque en español se denomina *"Registro de Nombre de Pasajeros"*.
[509] COM (2003) 826 final, de 16 de septiembre de 2003.
[510] COM (2010) 492 final, de 21 de septiembre de 2010.

nuevos acuerdos PNR con EE. UU[511] y Australia[512] en 2012. Estos acuerdos prevén la transferencia de datos PNR por parte de las compañías aéreas en los vuelos con destino y origen en la Unión Europea, de modo que dichos datos puedan utilizarse en la lucha contra el terrorismo y la delincuencia transnacional grave, al tiempo que incluyen salvaguardias para la protección de la intimidad y los datos personales. Las evaluaciones conjuntas de estos dos acuerdos se pusieron en marcha en el verano de 2019 para analizar su funcionamiento más amplio, su valor operativo y su necesidad.

En 2014, el Parlamento Europeo solicitó un dictamen al TJUE acerca de si el acuerdo previsto entre la UE y Canadá era compatible con los Tratados y la Carta de los Derechos Fundamentales y, como consecuencia de esta iniciativa, el proyecto de acuerdo no entró en vigor. El 26 de julio de 2017, el Tribunal de Justicia concluyó en el Dictamen 1/15[513] que el acuerdo no podía celebrarse como estaba previsto porque varias de sus disposiciones eran incompatibles con los derechos fundamentales reconocidos por la Unión, en particular el derecho a la protección de datos y el respeto a la vida privada. Tras el dictamen del Tribunal, en junio de 2018 se iniciaron nuevas negociaciones sobre el PNR con Canadá. En julio de 2019, ambas partes acogieron con satisfacción la conclusión satisfactoria de estas negociaciones y destacaron su compromiso de finalizar el acuerdo lo antes posible, a reserva de la revisión jurídica del texto por parte de Canadá[514]. Aunque el Dictamen 1/15 solo se refiere formalmente al acuerdo PNR previsto con Canadá, la Comisión está trabajando con sus otros socios internacionales para garantizar la conformidad de las transferencias internacionales de datos PNR con los Tratados y con la CDFUE, incluso en el contexto de las evaluaciones conjuntas de los acuerdos existentes mencionados anteriormente.

[511] Acuerdo entre los Estados Unidos de América y la Unión Europea sobre el tratamiento y la transferencia de datos de registro de nombre de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, OJ L 215, 11.8.2021, p. 5.

[512] Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por los transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia, OJ L 185, 14.7.2012, p. 4.

[513] Dictamen 1/15 del Tribunal de Justicia (Gran Sala), de 26 de julio de 2017, emitido con arreglo al artículo 218 TFUE, apartado 11, sobre el Proyecto de Acuerdo entre Canadá y la Unión Europea, en https://curia.europa.eu/juris/document/document/.jsf?text=&docid=193216&doclang=ES.

[514] Declaración conjunta de la Cumbre UE-Canadá, Montreal, 17-18 de julio de 2019.

En cuanto a otros terceros países, a raíz de una recomendación de la Comisión, el Consejo autorizó la apertura de negociaciones con Japón para la firma de un acuerdo PNR[515]. Las negociaciones con México, iniciadas en julio de 2015, están actualmente paralizadas.

El 6 de noviembre de 2007, la Comisión adoptó una propuesta de Decisión Marco del Consejo sobre la utilización de los datos del registro de nombres de los pasajeros (PNR) con fines represivos[516]. Tras la entrada en vigor del Tratado de Funcionamiento de la UE el 1 de diciembre de 2009, la propuesta de la Comisión, aún no adoptada por el Consejo, quedó obsoleta. En febrero de 2011, la Comisión presentó una propuesta de Directiva[517] que fue adoptada por el Parlamento Europeo y el Consejo en abril de 2016.

Como se ha señalado en párrafos precedentes, también en 2016, la UE modernizó su legislación en materia de protección de datos personales mediante la adopción del Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 -el antes denominado *"paquete de protección de datos"*. Estos actos legislativos garantizan la protección efectiva del derecho fundamental a la protección de datos consagrado en el Derecho primario[518]. Más recientemente, el 24 de junio de 2020, la Comisión adoptó una Comunicación sobre la adaptación de los antiguos instrumentos del Tercer Pilar [en el capítulo correspondiente, indicamos que la supresión de la estructura de tres pilares de la UE, por el Tratado de Lisboa, suponía un período de adaptación y reestructuración de materias, que todavía llega a nuestros días] a las normas de protección de datos[519] y

[515] Acuerdo PNR UE-Japón: El Consejo autoriza la apertura de las negociaciones, 18 de febrero de 2020, en https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/?utm_source?dsms-auto&utm_medium=email&utm_campaign=EU-Japan+PNR+agreement%3aCuncil+authorises+opening+of+negotiations

[516] COM (2007) 654 final, de 6 de noviembre de 2007.

[517] COM (2011) 32 final, de 2 de febrero de 2011.

[518] En particular, el Artículo 16 del TFUE garantiza el derecho a la protección de los datos. Este derecho está también consagrado en el Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

[519] COM (2020) 262 final, de 24 de junio de 2020.

publicó los resultados de la primera revisión y de la evaluación del Reglamento general de protección de datos de la Unión[520].

En este contexto, cabe señalar que el Tribunal Constitucional belga planteó una cuestión prejudicial al Tribunal de Justicia sobre la Directiva PNR[521]. El tribunal belga expresó dudas sobre la interpretación de determinadas disposiciones de la Directiva y su conformidad con la Carta de los Derechos Fundamentales. Poco después, el Tribunal de Distrito de Colonia también presentó una petición de decisión prejudicial[522]. El 21 de junio de 2022, el Tribunal de Luxemburgo dictó sentencia, mediante la que estimaba que el respeto de los derechos fundamentales exige que las facultades previstas por la Directiva PNR se limiten a lo estrictamente necesario. Nos detendremos aquí un poco más, por la relación de esta sentencia con las que afectan a la Directiva de Conservación de Datos.

El Tribunal de Justicia declara[523] que:

- La interpretación de las disposiciones de la Directiva PNR a la luz de los derechos fundamentales garantizados en los artículos 7, 8, 21 y 52, apartado 1 de la Carta garantiza la conformidad de la Directiva con esos artículos y el examen de las cuestiones planteadas no pone de manifiesto ningún elemento que pueda afectar a la validez de esta.

- Constata que la Directiva PNR comporta injerencias de una gravedad cierta en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta, ya que tiene por objeto la implantación de un régimen de vigilancia continuo, no selectivo y sistemático que incluye la evaluación automatizada de datos de carácter personal de todas las personas que utilizan servicios aéreos de transporte; y recuerda que la posibilidad de que los Estados miembros justifiquen tal injerencia debe apreciarse

[520] COM (2020) 264 final, de 24 de junio de 2020.

[521] Solicitud de una cuestión prejudicial en los casos conjuntos C-817/19 *Ligue des droits humains*, OJ C 36, 3.2.2020, p. 16-17

[522] Solicitud de una cuestión prejudicial en el Caso C-148/20, C-149/20 y C-150/20 *Deutsche Lufthansa.*

[523] Comunicado de prensa nº. 105/22, Sentencia del Tribunal de Justicia en el asunto C-817/19 Ligue des droits humains, Luxemburgo, 21 de junio de 2022, en https://curia.europa.eu/jcms/upload/application/pdf/2022-06/cp220105es.pdf

ponderando su gravedad y comprobando que la importancia del objetivo de interés general perseguido se corresponde con esta gravedad.

- Concluye que cabe considerar la recogida, la transferencia, el tratamiento y la conservación de datos PNR previstos en la Directiva se limitan a lo estrictamente necesario para luchar contra los delitos de terrorismo y los delitos graves, siempre que las facultades previstas por ella sean objeto de una interpretación restrictiva. En particular:
    i. Únicamente debe comprender las informaciones claramente identificables y delimitadas en las categorías que figuran en su anexo I y que guarden relación con el vuelo realizado y el pasajero de que se trate, lo que implica que, respecto de determinadas categorías de ese anexo, sólo estén cubiertas las informaciones contempladas expresamente.
    ii. La aplicación del sistema de la Directiva debe limitarse a los delitos de terrorismo y únicamente a los delitos graves que presenten un vínculo objetivo, cuando menos indirecto, con el transporte aéreo de pasajeros. La aplicación no puede extenderse a delitos que, pese a cumplir el criterio previsto por la Directiva relativo al umbral de gravedad y a pesar de quedar contemplados en su anexo II, forman parte de la delincuencia común con arreglo a las particularidades del sistema penal nacional.
    iii. La eventual extensión de la aplicación de la Directiva a todos o parte de los vuelos interiores de la Unión debe quedar limitada a lo estrictamente necesario y debe quedar sujeta al control efectivo de un órgano jurisdiccional o de un organismo administrativo independiente, cuyas resoluciones tengan efecto vinculante.

- En segundo lugar, el Tribunal se opone a una legislación nacional que autoriza el tratamiento de los datos PNR para fines diferentes de los expresamente indicados en su artículo 1.

- Respecto del plazo de conservación de los datos, el Tribunal se opone a que una legislación nacional que prevé una duración general de conservación de esos datos de cinco años se aplique a todos los pasajeros aéreos sin distinción. En

consecuencia, pasados seis meses, respecto de aquellos pasajeros sobre los que no se han revelado elementos objetivos que obliguen a conservar sus datos, su conservación no resulta limitada a lo estrictamente necesario. Hasta seis meses sí considera proporcionado y no excede de lo estrictamente necesario la conservación de los datos PNR de todos los pasajeros.

A nivel mundial, en diciembre de 2017 el Consejo de Seguridad de las Naciones Unidas adoptó la Resolución 2396 (2017), que exige a todos los Estados de la ONU que desarrollen la capacidad de recopilar, procesar y analizar los datos del PNR y que garanticen que los datos del PNR sean utilizados por todas sus autoridades nacionales competentes y compartidos con ellas, respetando plenamente los derechos humanos y las libertades fundamentales[524].

2.1 Respeto de los derechos fundamentales de los pasajeros

Uno de los objetivos clave de la Directiva es garantizar que el tratamiento de los datos por las autoridades se lleve a cabo de forma compatible con los derechos fundamentales de los pasajeros y, para ello, regula el modo en que los Estados miembros pueden utilizar los datos PNR y establece garantías para su protección. Solo nos referiremos a algunos aspectos concretos, a los que más relación tienen con el objeto de la tesis.

Respecto de la finalidad del tratamiento, los datos PNR solo pueden ser utilizados por los servicios policiales nacionales para prevenir, detectar, investigar y perseguir el terrorismo y los delitos graves[525]. La definición de los delitos de terrorismo se especifica aún más haciendo referencia a la Decisión Marco 2002/475/JAI[526], ahora sustituida por la Directiva (UE) 2017/541[527]. Se ha optado por reflejar en un anexo la

[524] Resolución 2396 (2017), adoptada por el Consejo de Seguridad en su reunión 8148, de 21 de diciembre de 2017.

[525] Artículo 1.2 de la Directiva (UE) 2016/681.

[526] Decisión Marco del Consejo 2002/475/JAI de 13 de junio de 2002, relativa a la lucha contra el terrorismo, OJ L 164, 22.6.2002, p. 3.

[527] Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se deroga la Decisión Marco 2002/475/JAI y se modifica la Decisión del Consejo 2005/671/JAI, OJ L 88, 31.3.2017, p. 6.

lista de delitos considerados graves y, para quedar bajo el ámbito de la Directiva, estos delitos tienen que estar penados con una pena máxima no inferior a tres años[528].

Respecto de la seguridad de los datos y el control de los accesos, la Directiva exige que los Estados miembros apliquen medidas técnicas y organizativas necesarias para garantizar que están sometidos a un alto nivel de seguridad[529] y que las operaciones de tratamiento quedan registradas y documentadas, de modo que una autoridad independiente con capacidad para ejercer el control pueda tener acceso a los registros en caso necesario, como podría ser a través de una auditoría. En la práctica, solo el personal que forma parte de las unidades que la Directiva prevé puede tener acceso directo a los datos recogidos (las Oficinas de Información de Pasajeros-PIUs; *PIU, por sus siglas en inglés*).

En relación con la conservación de los datos, el artículo 12, apartado 1 de la norma permite que puedan ser almacenados por las PIUs durante cinco años; sin embargo, después de seis meses deben *"enmascararse"*, eliminando todos los elementos que puedan servir para identificar a un pasajero. Los apartados 2 y 3 del artículo 12 establecen que:

"2. Al finalizar un plazo de seis meses desde la transmisión de datos PNR mencionada en el apartado 1, todos los datos PNR deberán ser despersonalizados mediante enmascaramiento de los siguientes elementos que podrían servir para identificar directamente al pasajero al que se refieren:

a) Nombre(s) y apellido(s), incluidos los de otros pasajeros que figuran en el PNR y número de personas que figuran en el PNR que viajan juntas;
b) Dirección y datos de contacto;
c) Todos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, o a cualquier otra persona;
d) Información sobre viajeros asiduos;

[528] Artículo 3.9 de la Directiva (UE) 2016/681.
[529] Artículo 13.7 de la Directiva (UE) 2016/681.

e) Observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, y

f) Toda la API recopilada" (Directiva PNR ,2016; L 119/143)".

3. "Al finalizar el período de seis meses mencionado en el apartado 2, solo se permitirá la divulgación de los datos PNR completos cuando:

a) Se crea razonablemente que es necesario a los efectos establecidos en el artículo 6, apartado 2, letra b), y

b) Haya sido aprobado por:

a. Una autoridad judicial, u

b. *Otra autoridad nacional competente para verificar si se cumplen las condiciones para la divulgación conforme al derecho nacional, con sujeción a la información y revisión a posteriori del responsable de la protección de la UIP."* (Directiva PNR, 2016; L 119/143).

Se observa que el legislador ha previsto que los datos despersonalizados puedan buscarse y divulgarse en el marco de investigaciones sobre actividades de terrorismo y de delincuencia grave, con la aprobación de las autoridades y siguiendo el procedimiento establecido.

Por otro lado, los pasajeros tienen derecho a acceder a sus datos, rectificarlos y hacer que se borren o se restrinja su tratamiento, así como a una indemnización por los daños que hayan sufrido y a recurrir a un tribunal[530]. Los Estados miembros deben garantizar que los pasajeros estén claramente informados sobre la recogida de datos PNR y sobre sus derechos[531].

[530] Artículo 13.1 de la Directiva (UE) 2017/681.

[531] La recogida y el tratamiento de datos PNR por parte de las compañías aéreas y sus proveedores de servicios, así como los derechos conexos de los interesados, están regulados por el Reglamento (UE) 2016/679 de protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, p. 1.

2.2 La necesidad y la proporcionalidad de la recogida y tratamiento de los datos PNR

El artículo 19 de la Directiva exige que la Comisión evalúe la necesidad y la proporcionalidad de la recogida y el tratamiento de los datos PNR para cada uno de los fines establecidos en ella, es decir: chequear a los pasajeros antes de su llegada o su salida de un país; responder a una solicitud debidamente motivada de las autoridades competentes, en el marco de investigaciones penales; y actualizar y crear los criterios predeterminados que se utilizarán para identificar a los pasajeros que requieran un control adicional por parte de las autoridades.

El tratamiento de datos que legitima la Directiva PNR tiene por objeto proteger la seguridad pública garantizando la prevención, la detección, la investigación y la persecución de delitos graves y del terrorismo en el espacio sin fronteras interiores existente en la Unión. Según confirmó el Tribunal de Justicia de la Unión Europea en su dictamen 1/15, el objetivo de garantizar la seguridad pública en la lucha contra los delitos de terrorismo y la delincuencia grave es un objetivo de interés general de la Unión capaz de justificar una injerencia, incluso grave, en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta[532]. En ese sentido, la Comisión entiende que esta conclusión también se puede aplicar a las operaciones de tratamiento de los datos PNR, que sirven para garantizar la seguridad pública en el territorio comunitario. Los datos PNR se utilizan en tiempo real para localizar a personas conocidas por su participación en actividades de terrorismo y delitos graves. Para lograrlo, los datos se cotejan automáticamente antes de la llegada o la salida con diversas bases de datos policiales de personas y objetos buscados. Estos datos pueden utilizarse también para identificar a personas implicadas en actividades delictivas o terroristas que todavía no son conocidas por las autoridades policiales, puesto que se pueden poner de manifiesto comportamientos de viaje atípicos o que se ajustan a pautas de viaje que suelen darse en el caso de delincuentes[533].

[532] Punto 149 del Dictamen 1/15 del TJUE.

[533] Los Estados miembros han facilitado a la Comisión algunos ejemplos que muestran bien la efectividad del almacenamiento y tratamiento de los datos PNR para el cumplimiento del objetivo previsto por la Directiva 2016/681.

El dictamen 1/15 también reconoció que, aunque el tratamiento de los datos PNR afecta a todos los pasajeros de los vuelos extracomunitarios entrantes y salientes, esa amplia cobertura es necesaria para alcanzar los objetivos previstos por la Directiva 2016/681, ya que *"la exclusión de determinadas categorías de personas, o de zonas de origen, podría obstaculizar la consecución del objetivo del tratamiento automatizado de los datos PNR"*, es decir, la identificación previa de las personas que pueden representar un riesgo para la seguridad pública *"entre todos los pasajeros aéreos"*[534]. Por otro lado, si bien es indudable que los datos PNR pueden *"revelar información muy específica"* sobre la vida privada de una persona, como reconoce el Tribunal de Justicia, *"la naturaleza de esa información se limita a determinados aspectos de la vida privada"*[535], en particular los relativos al transporte aéreo.

Sobre la recogida inicial de los datos, también en este caso[536], los datos PNR son recopilados inicialmente por las compañías aéreas para su uso comercial. El Considerando 8 indica que *"la Directiva no impone la obligación de recoger o conservar datos adicionales, ni obliga a los pasajeros a presentar datos más allá de los ya facilitados a las compañías aéreas"*. Considera la Comisión que,

> *"dado que los datos recogidos difieren en cada ocasión, el nivel de intrusión en la intimidad de las personas también varía y no debe equipararse en todos los casos al nivel máximo teóricamente posible en virtud de la Directiva, así como que la recogida de datos por parte de los transportistas aéreos es necesaria no sólo para la ejecución del contrato de transporte, sino también para satisfacer las necesidades o expectativas específicas de los pasajeros y, por lo tanto, al recurrir a los datos recogidos por los transportistas con fines comerciales, la Directiva PNR es menos intrusiva que una medida que obligara a los pasajeros a facilitar todos los datos que figuran en su anexo I"*[537].

[534] Punto 187 del Dictamen 1/15 del TJUE.
[535] Punto 50 del Dictamen 1/15 del TJUE.
[536] Como los datos a los que afecta la Directiva (UE) 2006/24/CE.
[537] Commission Staff Working Document accompanying the Report form the Commission to the European Parliament and the Council, on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM (2020) 305 final, p. 26

En cuanto al periodo de conservación de los datos PNR, el artículo 12, apartado 1 *obliga*[538] a los Estados miembros a conservar los datos PNR transferidos por las compañías aéreas durante cinco años, como indicamos antes. Este periodo de conservación se justifica por consideraciones objetivas relacionadas con el funcionamiento de los sistemas PNR y la naturaleza y duración de las investigaciones penales. En primer lugar, la necesidad de conservar los datos durante ese tiempo se deriva de la naturaleza del PNR como herramienta analítica destinada no sólo a identificar amenazas conocidas, sino también a descubrir riesgos desconocidos[539], que exige disponer de un conjunto de datos suficiente para un periodo relativamente largo[540] que evite errores o falsos positivos que, considera la Comisión, *"constituyen una mayor injerencia en los derechos fundamentales que el mero almacenamiento de los datos PNR en una base de datos de las UIPs"*[541].

Se justifica también una conservación tan larga para garantizar la investigación y el enjuiciamiento efectivo de los delitos de terrorismo y graves, con el argumento de que la investigación de estos delitos suele requerir meses y, a menudo, años de trabajo. En muchos casos, la investigación se refiere a actos cometidos con cierta antelación. Incluso si la detención se produce poco después del acto delictivo, puede revelarse que la misma persona podría haber participado en otras actividades delictivas y/o cooperar en su comisión con otras personas[542]. Además, la disponibilidad de los datos históricos garantiza que, cuando se acusa a una persona de haber cometido un delito grave o de estar implicada en actividades terroristas, es posible revisar el historial de viajes de la persona y ver con quién ha viajado, identificando a posibles cómplices u otros

[538] La obligación se expresa con la siguiente redacción del artículo 12.1: *"Los Estados miembros 'se asegurarán' de que los datos PNR proporcionados por las compañías aéreas a la UIP se conservan en una base de datos de la Unidad durante un plazo de cinco años a partir de su transmisión a la UIP del Estado miembro en cuyo territorio tenga su punto de aterrizaje u origen el vuelo".*

[539] Identificar patrones de comportamiento específicos y establecer asociaciones entre personas conocidas y desconocidas.

[540] En particular, los criterios predeterminados utilizados en el tratamiento automatizado de los datos PNR se reprograman y perfeccionan periódicamente para garantizar que sean específicos y proporcionados y evitar resultados falsos positivos, es decir, la notificación errónea de personas que no presentan ningún riesgo.

[541] Commission Staff Working Document, accompanying the *"Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681"*, p. 30.

[542] Una conexión con una organización terrorista o criminal solo puede detectarse cuando se dispone de más información, a medida que avanza una investigación o tras la comisión de un delito o atentado terrorista.

miembros de un grupo delictivo, así como a posibles víctimas[543]. Los datos históricos también pueden utilizarse para verificar la coartada de un sospechoso o para establecer de forma incuestionable que una pista no es lo suficientemente válida o fiable como para continuar con ella. Además, las salvaguardias previstas en la Directiva PNR en relación con el acceso de las autoridades competentes a los datos almacenados por las UIPs y en relación con la *"despersonalización y el desenmascaramiento"* de los datos tienen por objeto evitar los abusos. En particular, sólo se puede acceder a los datos históricos caso por caso, en respuesta a una solicitud debidamente motivada de las autoridades competentes y esta debe estar basada en motivos suficientes para que las autoridades competentes traten los datos PNR, en relación con un caso concreto, a efectos de la Directiva. Tras la despersonalización, la plena divulgación (desenmascaramiento) de los datos PNR requiere una autorización de una autoridad judicial o administrativa habilitada para esta función, que debe ir precedida del análisis de la necesidad de dicha divulgación a efectos de prevenir, detectar, investigar y perseguir delitos graves.

Por último, en lo que respecta a los plazos de conservación de los datos que deben transmitirse a Canadá, considerados por el Tribunal de Justicia en el Dictamen 1/15, es importante señalar que la realización de controles fronterizos no es una finalidad de la Directiva PNR, que busca claramente el objetivo de garantizar la seguridad en la Unión y su espacio sin fronteras interiores, donde los Estados miembros comparten la responsabilidad de garantizar la seguridad pública.

Del mismo modo, la naturaleza de la Directiva PNR como derecho derivado significa que su aplicación está rodeada de las garantías adicionales intrínsecas al acervo, y por tanto tiene lugar bajo el control de los tribunales nacionales de los Estados miembros y, en última instancia, del Tribunal de Justicia.

[543] Las autoridades nacionales también han informado de que, en algunos casos, el análisis de datos históricos del PNR ha sido la única herramienta disponible para establecer o probar los vínculos entre las personas implicadas en la comisión de un delito.

2.3 Alcance/limitación de la finalidad restrictiva

Ya hemos citado los usos previstos de los datos del PNR (prevenir, detectar, investigar y perseguir los delitos de terrorismo y los delitos graves enumerados en el anexo II) que estén penados según lo previsto en el artículo 3.9[544]. Los Estados miembros han informado a la Comisión de que la limitación de la finalidad de la Directiva no siempre se corresponde con las importantes necesidades operativas y los retos a los que se enfrentan las autoridades policiales en su trabajo diario. En particular, el limitado ámbito de aplicación dificulta la cobertura de determinadas actividades delictivas que, tomadas aisladamente, pueden parecer menores, pero que en realidad están vinculadas a la delincuencia organizada grave[545]. Consideran también los servicios policiales de los Estados miembros que los datos PNR podrían desempeñar un papel vital para alcanzar ciertos objetivos importantes que actualmente no están cubiertos por la Directiva. En particular, el sistema PNR podría constituir una valiosa herramienta para el seguimiento de personas desaparecidas -incluidos los menores- o para la protección de la salud pública. Creen también que el ámbito de aplicación es más restringido que el de otros instrumentos de la UE relacionados con la cooperación policial, como la orden europea de detención (OED)[546] o el Sistema de Información de Schengen (SIS). La OED se aplica a todos los tipos de delitos y puede ser emitida por una autoridad judicial nacional si la persona buscada está acusada de un delito cuya pena máxima es de al menos un año de prisión o ha sido condenada a una pena de prisión de al menos cuatro meses[547]. Para una lista de treinta y dos delitos graves castigados con penas de privación de libertad de al menos tres años, la entrega de la persona no requiere la comprobación de la doble incriminación del hecho[548]. Esta lista coincide en gran medida con la lista establecida en el anexo II de la Directiva PNR, pero no es exactamente igual. Dado que el SIS incluye entre sus categorías de descripción a las personas sobre las que se ha dictado una orden de europea de detención[549], estas

[544] Artículo 3.9 de la Directiva PNR: "*A efectos de la presente Directiva, se entenderá por: […] 9) 'delitos graves': los delitos incluidos en el anexo II que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo al derecho nacional de un Estado miembro"*.

[545] Por ejemplo, las redes de carteristas en las que también puede haber un elemento de trata de seres humanos.

[546] Decisión marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros - Declaraciones de algunos Estados miembros con motivo de la adopción de la Decisión marco DO L 190 de 18.7.2002, p. 1.

[547] Artículo 2.1 de la Decisión Marco 2002/584/JAI del Consejo.

[548] Artículo 2.2 de la Decisión Marco 2002/584/JAI del Consejo.

[549] Artículo 26 de la Decisión 2007/533/JAI del Consejo.

diferencias en el ámbito de aplicación pueden dar lugar a que los datos del PNR-SIS resulten en coincidencias con delitos que no entran en el ámbito de aplicación de la Directiva PNR.

En consecuencia, algunos Estados miembros consideran que las limitaciones actuales son incoherentes con la lógica general del marco de cooperación policial de la UE y han señalado la necesidad de ampliar el ámbito de aplicación de la Directiva PNR. Esto podría lograrse, en particular, mediante la inclusión de más delitos en el anexo II, para hacerlos coherentes, por ejemplo, con la OED. Sorprende que, en el caso del sistema PNR, la posición de los expertos de los Estados miembros es pedir más por considerar que se puede obtener más rendimiento del sistema; no obstante, la situación respecto de la conservación de datos de las comunicaciones electrónicas es radicalmente diferente, y los expertos están buscando alguna razón que convenza al TJUE de la necesidad de volver al sistema del 2006 o reducir al mínimo el impacto de su derrumbamiento. En cambio, las similitudes entre ambas situaciones son más que las diferencias. Intentaremos extraer alguna conclusión al respecto.

CAPÍTULO VIII. EL CAMBIO DE PARADIGMA INTRODUCIDO POR EL TRIBUNAL EUROPEO

A raíz de la decisión del Tribunal de Justicia declarando la invalidez *ex tunc* de la Directiva de 2006, *sonaron las alarmas* en los Estados miembros, aduciendo que se dificultaría la realización eficaz de las investigaciones penales y, en 2017, se puso en marcha un proceso de reflexión en el seno del Consejo de la UE sobre cómo avanzar[550] y con el objetivo de explorar posibles soluciones para garantizar la disponibilidad de datos con fines de prevención y lucha contra la delincuencia. El Consejo de la Unión Europea valoró entonces los efectos de la sentencia y consideró que no había más remedio que realizar una evaluación estricta de la proporcionalidad y de la necesidad de las medidas que se adopten, pero nunca podrían estas constituir graves restricciones de los derechos fundamentales, aunque sean legítimos los objetivos perseguidos; así como que debían establecerse salvaguardias adecuadas respecto de las medidas de conservación que se aprueben[551].

A efectos prácticos, se puede considerar [y así se entendió] que el Tribunal insta a las instituciones europeas y los Estados miembros a proponer y aprobar un nuevo sistema de conservación de datos que sea respetuoso con los derechos consagrados en la Carta. El hecho de que sea la primera vez que el Tribunal de Luxemburgo declara inválida una Directiva en su totalidad y con efectos retroactivos, además de reforzar su posición como guardián de los ciudadanos europeos, lanza un mensaje muy contundente a los decisores políticos sobre la gravedad de la injerencia a los derechos de los ciudadanos que habían aprobado con esta decisión. De hecho, como ya indicamos anteriormente, los magistrados que dictaron la sentencia no siguieron el criterio del Abogado General, que había planteado en sus Conclusiones que la invalidez quedara

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

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

suspendida en sus efectos[552] hasta que se adoptaran otras medidas por parte de las instituciones europeas para su ejecución; otro hecho poco habitual, puesto que el Tribunal suele seguir el criterio que apunta el Abogado General. Tampoco siguió el Tribunal el criterio del Abogado General en cuanto a que los Estados miembros pudieran *subsanar* la invalidez a través de las normativas de transposición; al contrario, se obliga a replantear todo el sistema europeo de conservación de datos, aunque se dejan algunas opciones para llevarlo a efecto, con poca concreción.

Es cierto que con el paso del tiempo los cuerpos policiales han ido adaptando sus métodos y técnicas de investigación para el esclarecimiento de los delitos y, en la sociedad de la información en que vivimos, con una *excesiva* interdependencia y conectividad entre los ciudadanos, las autoridades han tenido que reaccionar [muchas veces tarde o demasiado lento] para poder aprovechar la ingente cantidad de información que se genera y se comparte, también a esos fines de esclarecimiento y enjuiciamiento de los delitos, hasta el punto que para algunos autores se ha llegado a una situación de *"tecnovigilancia"*[553] y se ha avanzado a un ritmo desigual entre el empleo de técnicas de investigación de este tipo y la elaboración de una legislación adecuada y actual en la materia que respalde esa actuación. Quizás esta dependencia justifica en parte la gravedad de la situación creada por el Tribunal europeo, hasta el punto de que ha supuesto una labor difícil y, hoy en día, no muy productiva, para poder aprobar una nueva normativa europea sobre la conservación y acceso a los datos de las comunicaciones electrónicas que sea conforme con la jurisprudencia del Tribunal europeo y satisfaga las necesidades de los ciudadanos, respecto de las misiones que estos han adjudicado a las agencias encargadas de la aplicación de la ley.

Y no es solo es una situación con implicaciones negativas en la capacidad de investigación y persecución de delitos graves que hayan puesto de manifiesto las Fuerzas y Cuerpos de Seguridad, sino también el ministerio fiscal -al menos en España-.

[552] El artículo 266 del TFUE prevé que *"la institución, órgano u organismo del que emane el acto anulado, o cuya abstención haya sido declarada contraria a los Tratados, estará obligado a adoptar las medidas para la ejecución de la sentencia del Tribunal de Justicia de la Unión Europea"*.

[553] ORTIZ-PRADILLO, J.C., *"Europa: Auge y caída de las investigaciones penales…"*, op. cit., p. 10.

En ese sentido, cita Ortiz-Pradillo (2020; 14)[554] la Circular 1/2013 de la Fiscalía General del Estado[555], que alertó de los efectos negativos de una interpretación restrictiva del concepto de delito grave, puesto que las consecuencias sobre la investigación de determinadas conductas penales serían notorias y *"supondría cortar de raíz la posibilidad de investigar conductas que utilizando tecnologías de la información y la comunicación y teniendo gran transcendencia social, no alcanzan por la penalidad asignada el rango de delito grave"*. Propone la Fiscalía española *"sustituir la expresión 'delito grave' por otra que delimite el perímetro de aplicación de la Ley [Ley 25/2007] en términos más amplios y razonables"*. Sin embargo, no hemos encontrado propuesta concreta que cumpla con los requisitos que revela la fiscalía general.

Tras las primeras reflexiones y debates a nivel de expertos, en un informe presentado ante el Consejo JAI en diciembre de 2018 (durante la Presidencia austriaca del Consejo), se sometió al parecer de los ministros un documento en el que se exponían las conclusiones de ese proceso de reflexión y el estado de los trabajos sobre la conservación de datos a efectos de aplicación de la ley. Los mandatarios debatieron sobre futuras actuaciones y respaldaron la continuación de los trabajos a nivel de los técnicos a fin de estudiar vías para determinar un planteamiento en relación con la conservación de datos en el seno de la Unión.

Posteriormente, los debates organizados por la Presidencia rumana sobre la posible dirección futura desembocaron en las Conclusiones del Consejo de junio de 2019. Se encomendó a la Comisión que emprendiera consultas específicas con los interesados y llevara a cabo, sobre esa base, un estudio comparativo en materia de conservación de los datos que tuviera en cuenta las distintas opciones, incluida la preparación de una nueva propuesta legislativa. El estudio concluyó en otoño de 2020[556].

[554] *Ibíd.*,. p. 14.

[555] Circular 1/2013, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, de la Fiscalía General del Estado, en https://www.boe.es/buscar/abrir_fiscalia.php?=id=FIS-C-2013-00001.pdf

[556] Vid. WK 11460/2020 INIT, Study on the retention of electronic communications non-content data for law enforcement purposes, final report, de 22 de octubre de 2022.

Ese mismo año, en octubre de 2020, el Tribunal dictó nuevas sentencias en una serie de asuntos acumulados[557] que ya hemos analizado y que, como hemos puesto de manifiesto, confirmaban la ilicitud de la conservación generalizada e indiscriminada de datos y establecía excepciones a ese principio, que los Estados miembros están todavía en este momento analizando, quizás en un punto muerto, por falta de ideas claras sobre cómo afrontar la situación y por diferencias de criterio sobre qué modificar y qué mantener, basándose en criterios [a nuestro modo de ver] puramente nacionales y no europeos.

También en ese mismo año, en las Conclusiones del Consejo Europeo de diciembre de 2020[558], se reconocía que *"es esencial que las autoridades policiales y judiciales puedan ejercer sus competencias legales para combatir la delincuencia grave tanto en Internet como fuera de Internet"*. En este sentido, *"el Consejo Europeo resalta la necesidad de avanzar en los trabajos relativos a la conservación de datos necesaria para luchar contra la delincuencia grave, a la luz de la jurisprudencia más reciente del Tribunal y respetando plenamente los derechos y libertades fundamentales"*. Este apoyo político es importante, puesto que muestra que los jefes de estado y de gobierno siguen siendo conscientes de la magnitud del problema y mantienen de forma unánime el interés por buscar una solución satisfactoria para todas las partes; sin embargo, indica también que el cambio introducido por el Tribunal es muy complejo, como se ha confirmado con el hecho claro de que, varios años después de comenzar las reflexiones, aún no se vislumbra solución concreta y aceptada por todas las partes.

Posteriormente, en la orientación general del Consejo de comienzos febrero de 2021 en torno a la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas[559], se trataban varios aspectos relacionados con la conservación de datos, como la exclusión del ámbito de aplicación de ese reglamento del tratamiento de estos a

[557] Sentencias de 6 de octubre de 2020: asuntos acumulados C-511/18, C-512/18 y C-520/18; y asunto C-623/17.

[558] Vid. EUCO 22/20, consultado en https://www.consilium.europa.eu/media/47348/1011-12-20-euco-conclusions-es-pdf, consultada el 14.07.21, p.9.

[559] Documento 5840/21 del Consejo de la Unión Europea, que contiene la orientación general de esta institución europea respecto del borrador de Reglamento del Parlamento Europeo y del Consejo relativo al respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas y por la que se deroga la Directiva 2002/58/CE (Reglamento de privacidad y las comunicaciones electrónicas).

efectos de la seguridad nacional, e introducía una referencia explícita a la conservación de datos con fines policiales y de seguridad pública. Nos detendremos en este aspecto, por su importancia, ya que esta norma europea (en fase de tramitación, pero que ya ha alcanzado un acuerdo en la propuesta del Consejo, y que deberá ahora negociar con el Parlamento Europeo) sustituirá a la Directiva de 2002, que es actualmente la que da soporte a las medidas que se adopten respecto de la conservación de datos de las comunicaciones electrónicas. En consecuencia, parece muy oportuno resaltar aquellos artículos que recoge el borrador de la nueva norma respecto de las excepciones al régimen general de privacidad de las comunicaciones electrónicas (recordemos que ahora, como hemos repetido numerosas veces, una vez anulada la Directiva 2006/24/CE, es el artículo 15, apartado 1 de la Directiva de 2002 el que establece las excepciones).

El futuro reglamento, si es aprobado con la redacción actual de la orientación general del Consejo (no es probable que se respete íntegramente, puesto que el Parlamento suele introducir numerosas enmiendas y, aunque tampoco se aceptan todas, no nos equivocaremos si aventuramos que alguna se propondrá respecto de los artículos que citaremos continuación), regularía las excepciones a la norma a través de los siguientes artículos:

- *Artículo 7.4*, relativo al almacenamiento y borrado de datos de las comunicaciones electrónicas, recoge que: *"El Derecho de la Unión o de los Estados miembros podrá prever, de conformidad con el artículo 11, que los metadatos de las comunicaciones electrónicas se conserven para salvaguardar la prevención, la investigación, la detección o el enjuiciamiento de los delitos o la ejecución de las sanciones penales, así como la protección y la prevención de las amenazas a la seguridad pública, durante un período limitado que podrá prorrogarse si persisten las amenazas a la seguridad pública de la Unión o de un Estado miembro".*

- *Artículo 11* (correspondería al actual artículo 15, apartado 1), relativo a restricciones: *"El Derecho de la Unión o de los Estados miembros podrá restringir mediante una medida legislativa el alcance de las obligaciones y los derechos previstos en los artículos 5 a 8 cuando dicha restricción respete la esencia de los derechos y libertades fundamentales y sea una medida necesaria, adecuada y*

proporcionada en una sociedad democrática para salvaguardar uno o varios de los intereses públicos generales a que se refiere el artículo 23, apartado 1, letras c) a e), i) y j), del Reglamento (UE) 2016/679 o una función de control, inspección o reglamentación relacionada con el ejercicio del poder público para dichos intereses. El artículo 23, apartado 2, del Reglamento (UE) 2016/679 se aplicará a cualquier medida legislativa mencionada en el apartado 1.

Los proveedores de servicios de comunicaciones electrónicas establecerán procedimientos internos para responder a las solicitudes de acceso a los datos de comunicaciones electrónicas de los usuarios finales basadas en una medida legislativa adoptada de conformidad con el apartado 1. Facilitarán a la autoridad de control competente, previa solicitud, información sobre dichos procedimientos, el número de solicitudes recibidas, la justificación invocada y su respuesta".

- El artículo 2.2 (a) y 2.2 (d), relativos a las excepciones a la aplicación del reglamento, recogen respectivamente: *"2.2 (a) las actividades que quedan fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, las medidas y operaciones de tratamiento relativas a la seguridad y la defensa nacionales, independientemente de quién las lleve a cabo; y 2.2 (d) actividades, incluidas las actividades de tratamiento de datos, de las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluida la salvaguardia y la prevención de amenazas a la seguridad pública".*

- El artículo 6.1 (d), relativo al tratamiento permitido de los datos de las comunicaciones electrónicas, recoge que: *"los proveedores de redes y servicios de comunicaciones electrónicas sólo podrán tratar los datos de las comunicaciones electrónicas si: (d) es necesaria para el cumplimiento de una obligación legal a la que está sujeto el prestador establecida por el Derecho de la Unión o de los Estados miembros, que respeta la esencia de los derechos y libertades fundamentales y es una medida necesaria y proporcionada en una sociedad democrática para salvaguardar la prevención, la investigación, la detección o el*

enjuiciamiento de delitos o la ejecución de sanciones penales, así como la salvaguardia y la prevención de amenazas a la seguridad pública".

Observamos que el borrador recoge, con una redacción diferente e incluyendo referencias al Reglamento General de Protección de Datos de la Unión Europea, menciones concretas a la posibilidad de establecer límites a su contenido y permitir una futura norma europea de conservación de datos respetuosa con los derechos y libertades fundamentales de los ciudadanos europeos. Lo relevante del texto es que, la modificación del régimen de privacidad de las comunicaciones electrónicas no cierra la puerta a la adopción de medidas legislativas (europeas o nacionales) para regular la conservación de los datos; eso sí, no cambia nada en el hecho, ahora constatado por el Tribunal europeo, de que esas medidas son una excepción a lo previsto en el futuro reglamento y que deberá cumplir con los criterios jurisprudenciales establecidos por el TJUE. Aunque no se menciona que la habilitación para la adopción de medidas en el ámbito de la investigación penal tendrá que serlo solo para los delitos graves, la propia doctrina del Tribunal ya ha dejado claro los diferentes supuestos y las medidas que se podrán adoptar en uno u otro caso, además de las garantías y salvaguardas precisas para ello.

Tras este inciso sobre el estado de situación de la futura norma de privacidad de las comunicaciones electrónicas, seguimos el repaso cronológico con las distintas respuestas al estado de alarma provocado por la invalidación del sistema de conservación de datos del 2006.

En la reunión del Comité de Coordinación en el ámbito de la Cooperación Policial y Judicial en Materia Penal (CATS) celebrada el 8 de febrero de 2020, varios Estados miembros apoyaron la adopción de legislación europea que armonizara el régimen jurídico y propusieron que este asunto se debatiera a nivel político en el Consejo JAI del 11 de marzo de ese año, esta vez a nivel de ministros de justicia y no de interior. Los ministros intercambiaron impresiones sobre la conservación de metadatos en las comunicaciones electrónicas y hubo un amplio apoyo a la idea de explorar las

posibilidades de una nueva legislación europea en materia de conservación, aunque otros creyeron necesario continuar con las discusiones sobre cómo cumplir con la jurisprudencia del Tribunal europeo antes de avanzar hacia un nuevo escenario; en definitiva, no había suficientes elementos sobre la mesa como para tener clara la forma de proceder y, ante esa situación [como ocurre habitualmente en toda negociación, pero más aún cuando los negociadores son muchos, aunque pertenezcan al mismo grupo o colectivo. En este caso correspondía al Consejo de la Unión Europea y todavía no tiene una posición común] se optó por seguir reflexionando e intercambiando puntos de vista e impresiones, sin una dirección clara de quién, a nuestro juicio, debía haber tenido un papel más activo: la Comisión Europea.

Durante todo este tiempo, el Parlamento Europeo, como colegislador con el Consejo de la UE en la mayoría de los expedientes legislativos a nivel de la Unión, también se ha pronunciado de forma reiterada. El 17 de diciembre de 2020, adoptó una resolución sobre la Estrategia de la Unión Europea para una Unión de la Seguridad[560] en la que señala lo que ya era perfectamente conocido: en las sentencias de octubre de 2020, el TJUE confirmó la jurisprudencia anterior, concluyendo que *"solo se permite una retención selectiva de datos limitada a personas concretas o a una zona geográfica específica"*, pero también apostilló que *"las direcciones IP asignadas a la fuente de una comunicación pueden ser objeto de una retención generalizada e indiscriminada con el fin de luchar contra la delincuencia grave y las amenazas graves para la seguridad pública, con estrictas garantías"*. El Parlamento adoptó una resolución de fecha 26 de noviembre de 2020 sobre la situación de los derechos fundamentales en la UE en 2018-2019[561], en la que *"pide a la Comisión Europea que inicie procedimientos de infracción contra los Estados miembros cuyas leyes de aplicación de la Directiva de retención de datos invalidada no han sido derogadas para adaptarlas a la jurisprudencia del Tribunal europeo"*. En su resolución de 12 de diciembre de 2018 sobre las conclusiones y recomendaciones del Comité Especial sobre el Terrorismo[562],

[560] Estrategia de la UE para la Unión de la Seguridad, P9_TA(2020)0378, consultada el 14.04.21 en https://www.europarl.europa.eu/doceo/document/TA-9-2020-0378_ES.pdf. Letra M.

[561] Situación de los derechos fundamentales en la Unión Europea: informe anual para los años 2018 y 2019. P9_TA(2020)0328, consultado en https://www.europarl.europa.eu/doceo/document/TA-9-2020-0328_ES.pdf , el 14.04.21

[562] Conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo. Resolución del Parlamento Europeo, de 12 de diciembre de 2018, sobre las conclusiones y recomendaciones de la

esta institución también se había posicionado al respecto e instó *"a la Comisión a evaluar la propuesta legislativa sobre la conservación de datos que respete los principios de limitación de la finalidad, proporcionalidad y necesidad, teniendo en cuenta las necesidades de las autoridades competentes y las especificidades del ámbito de la lucha contra el terrorismo"*.

Volviendo al Consejo, en este caso en la reunión del Consejo Europeo de fecha 25 de marzo de 2021, los jefes de estado y de gobierno[563] hicieron un llamamiento a sus respectivos países para:

> *"aprovechar mejor el potencial de los datos y las tecnologías digitales en beneficio de la sociedad, el medio ambiente y la economía, respetando al mismo tiempo la protección de los datos pertinentes, la intimidad y otros derechos fundamentales, y garantizando la conservación de los datos necesarios para que las autoridades policiales y judiciales ejerzan sus competencias legales en la lucha contra la delincuencia grave"*.

Posteriormente, en la Estrategia contra la Delincuencia Organizada de 14 de abril de 2021[564], la Comisión Europea anunció que analizaría y esbozaría posibles enfoques y soluciones, en consonancia con las sentencias del Tribunal, *"que respondieran a las necesidades policiales y judiciales de una manera que fuera útil desde el punto de vista operativo, técnicamente posible y jurídicamente sólida, incluido el pleno respeto de los derechos fundamentales, a fin de idear el camino a seguir"*. En este caso, quizás porque el proceso de reflexión estaba en un punto muerto, la Comisión mostró [al menos sobre el papel] una actividad más proactiva y (respondiendo a los llamamientos de los Estados miembros, a través del Consejo de la Unión Europea y de las reuniones de los máximos representantes de los Estados, a través del Consejo

---

Comisión Especial sobre Terrorismo (2018/2044(INI)), consultado el 14.04.21, en https://www.europarl.europa.eu/doceo/document/TA-8-2018-0512_ES.pdf

[563] Documento SN 18/21, de 25 de marzo de 2021, consultado el 15.04.21, en https://www.consilium.europa.eu/media/49007/250321-vtc-euco-statement-es-pdf.

[564] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2021) 170 final, de 14.4.2021.

Europeo) apostó por aportar distintas propuestas que enfocaran el problema y mostraran alternativas concretas sobre las que debatir.

En esta accidentada carrera de obstáculos propiciada por el Alto Tribunal europeo, hasta la fecha todo han sido dificultades: por un lado, la correspondiente al acceso limitado a los datos y, por otro (y quizás más grave, por cuanto sin este paso no se puede producir el anterior), la relativa al establecimiento de la forma de conservación (la conservación selectiva). Mientras tanto, los cuerpos policiales comprueban como se desmorona uno de los elementos de investigación principales ante muchos delitos. Ortiz-Pradillo (2020; 11)[565] considera que es difícil encontrar una solución al problema si ha de venir únicamente a través de la vía interpretativa y no mediante una nueva propuesta legislativa en los Estados miembros. Nosotros no estamos todavía en disposición de llegar a esa conclusión, ni cualquiera otra: quizás la vía interpretativa pueda arrojar luz; o, por qué no, una nueva propuesta legislativa europea; o la adopción de soluciones individuales a nivel de los Estados miembros; o unas orientaciones generales de la Comisión, sin efecto vinculante, pero que intenten armonizar los criterios a seguir por los Estados miembros, etcétera.

Sí que podemos mencionar algunos casos prácticos que se pusieron encima de la mesa en los primeros debates entre expertos en investigación de los Estados miembros, convocados por Europol en 2017, donde se ilustraron algunos ejemplos de suficiente entidad como para mostrar preocupación respecto de en qué medida podría afectar negativamente a la protección de los ciudadanos ante delitos graves para cuyo esclarecimiento son necesarios los metadatos sobre los que la Directiva 2006/24/CE había establecido un régimen de conservación y de puesta disposición de las agencias encargadas de la aplicación de la ley.

Y es que, como sabemos, actualmente los datos electrónicos (como las direcciones IP) son a menudo el punto de partida de una investigación, lo que significa que los datos necesarios y las posibles pruebas nacen digitalmente. Estos casos no

[565] ORTIZ-PRAILLO, J.C., *"Europa: Auge y caída de las investigaciones penales…"*, op. cit. p. 11.

pueden resolverse normalmente mediante el *trabajo policial clásico* o incluso mediante la inversión en más recursos humanos o materiales; es imprescindible contar también un marco regulador que permita aprovechar el potencial de uno de los bienes más preciados de la sociedad actual: la información (en este caso en forma de datos de las comunicaciones electrónicas).

Se explicó un caso de propaganda antiterrorista en el que se establecieron más de 2.000 conexiones IP en 19 Estados miembros diferentes de la UE y no se pudo llegar hasta los sospechosos porque los registros de las IP que contenían la información relevante para la investigación ya no estaban almacenados por los proveedores de servicios de Internet.

Otra situación frecuente se produce en el marco de investigaciones complejas de delincuencia organizada o ante la comisión de un atentado terrorista, en las que los investigadores tratan de identificar a las víctimas, a los autores/sospechosos (fallecidos) y a los posibles sospechosos en libertad. En estos escenarios, la clave del éxito está en: *i) la rapidez con la que se obtenga la información pertinente; ii) la exactitud de los datos conservados con vistas a orientar adecuadamente la investigación en un breve plazo de tiempo; y iii) en separar el grano de la paja*, es decir, la posibilidad de extraer información pertinente entre una cantidad ingente de datos. El análisis de tipo forense para realizar esa acción de extracción puede llevar mucho tiempo y consumir muchos recursos, especialmente si los datos están encriptados o si el número de solicitudes se multiplica, debido al número de dispositivos, proveedores y países implicados; así como si es necesario acudir a los mecanismos de cooperación policial internacional y solicitar, pongamos por caso, comisiones rogatorias internacionales por vía judicial y diplomática.

Relataremos a continuación, de forma somera, otras situaciones ficticias y genéricas, pero factibles que nos permitan ilustrar o visualizar situaciones concretas y la importancia de los datos que estamos estudiando:

- Una *investigación previa a un atentado terrorista* en la que fue necesaria una vigilancia sobre un grupo de sospechosos que planeaba cometer un atentado terrorista en la Unión Europea. En este caso, como en cualquier otro de estas características, los investigadores tenían que identificar a los posibles autores y su red de apoyo (logística, finanzas, etcétera) y llegar a conocer dónde y cuándo tenía previsto este grupo cometer el atentado.

  Durante la investigación, se recoge información de diversas fuentes, como manifestaciones de testigos presenciales, pruebas obtenidas en el lugar del delito (documentos de identidad, huellas dactilares, etc.), datos de vigilancias (matrículas, direcciones de reuniones, etcétera), averiguación de datos (números de teléfono, cuentas bancarias, etcétera), datos extraídos mediante examen forense de diferentes dispositivos digitales, contenido y metadatos de fuentes disponibles públicamente (por ejemplo, plataformas de comunicación como Internet, Darknet, etcétera), y contenido y metadatos de fuentes no disponibles públicamente (CCTV, etcétera).

  Centrándose en los identificadores únicos contenidos en estas fuentes de datos, los investigadores trazan la huella online y offline del sospechoso o sospechosos. Para ello, también se tiene en cuenta la información sobre la logística, medios de comunicación, centro de interés/comportamiento, medios financieros y relaciones de estos. Esos identificadores podrían incluir también otros no basados en Internet pero sí en otros medios de comunicación electrónica, como números de teléfono, datos de abonados, de facturación, de conexión con los repetidores, u otra información asociada como los detalles de los abonados, los datos de la conexión celular GSM, etcétera; correo electrónico, números de teléfono, apodos, avatares [imágenes], identificadores financieros (números de tarjetas de crédito, correo electrónico, ID de transacciones de bitcoin, etcétera) e identificadores logísticos (matrículas, direcciones, etcétera).

  Por lo que respecta a la huella en línea, esta información suele estar dispersa en diferentes proveedores de servicios situados en varias jurisdicciones dentro y fuera de la Unión. Además, la Información Básica del Suscriptor *(BSI, por sus siglas en inglés)* está a veces vinculada a identidades falsas, medios de pago anónimos, y

proxies e IPs cubiertas que permiten a los delincuentes ocultar su dirección IP real. Sin embargo, todos estos identificadores contienen marcadores que pueden ser de interés para la investigación.

En consecuencia, dependiendo de la necesidad operativa, se pueden solicitar tres tipos de datos: la divulgación urgente de BSI, los datos de tráfico o los datos de contenido. Aunque las BSI y los datos de tráfico pueden proporcionar información parcial (principalmente sobre logística, medios de comunicación, centro de interés/comportamiento), por lo general no permitirán identificar al sospechoso o al autor. Además, los datos de contenido pueden proporcionar información parcial también sobre los medios financieros y las relaciones. Sin embargo, cualquier análisis de posibles pistas se beneficia de la correlación de los tres tipos de datos y de su cotejo con la información existente en las bases de datos propias de los servicios policiales y de inteligencia, por lo que centrarse en un solo tipo de datos conlleva el riesgo de que se produzcan falsos positivos, es decir, falsas alarmas en un contexto en el que cualquier hallazgo contribuye al esclarecimiento del hecho que se investiga, así como disminuye el riesgo de que se pierdan datos críticos; lo que puede ser determinante en el caso en que se esté preparando un atentado.

- Una *investigación por la comisión de un atentado terrorista* en un Estado miembro, que causó víctimas y en el que fallecieron también los autores. Los servicios policiales recopilaron información de testimonios en directo, pruebas en el lugar del atentado (documentos de identidad, huellas dactilares, etcétera), datos forenses en el lugar de los hechos (extracción de datos de un teléfono móvil encontrado en el lugar del atentado y todavía encendido), datos extraídos mediante examen forense de diferentes dispositivos digitales, contenido y metadatos de fuentes disponibles públicamente en línea (Periscope, Twitter, Facebook, etcétera), y contenido y metadatos de fuentes no disponibles públicamente (CCTV, etcétera) para extraer los identificadores únicos asociados. Al igual que en el caso anterior, para identificar a los autores y a los sospechosos en libertad, los investigadores necesitaban trazar su huella en línea y fuera de línea.

La identificación de la(s) víctima(s) debía ser lo más rápida posible. Dado que las víctimas no son sospechosas de utilizar identidades falsas cuando se suscriben a proveedores de servicios en línea, la BSI suele ser suficiente para su identificación. Si no da ningún resultado, se solicitaría posteriormente información sobre el contenido. Además, habrá que identificar y posiblemente localizar a los autores (fallecidos) y a los sospechosos en libertad. Ambos objetivos están estrechamente relacionados: en varios casos, la identificación del primero lleva al segundo. Para completar la investigación, se requiere de nuevo el mapeo de su huella online y offline, incluyendo todos los tipos de datos.

- Los siguientes casos ilustran algunos de los puntos de partida típicos de las investigaciones sobre ciberdelincuencia:
  a) *Online moniker*: después de recuperar un nombre/apodo de, por ejemplo, un foro clandestino en el contexto de una investigación, el siguiente paso implicaría un cotejo del nombre con los datos existentes en las bases policiales y complementar los datos utilizando fuentes disponibles públicamente (OSINT). Esto puede llevar a una situación en la que se pueda identificar una dirección de correo electrónico (o cualquier otro identificador en línea, por ejemplo, Skype, Jabber[566], ICQ[567], perfil de medios sociales) que esté asociado a este apodo.

A continuación, se enviaría una solicitud al proveedor de correo electrónico y/o a la plataforma en línea (en el caso de un foro). De la respuesta del proveedor de correo electrónico o de la plataforma, los investigadores pueden recibir las IP de inicio de sesión, potencialmente otra dirección de correo electrónico (utilizada como correo de recuperación, por ejemplo) y un número de teléfono móvil (si el foro o la plataforma utiliza la autenticación de dos factores). El proceso comenzaría entonces de nuevo con comprobaciones cruzadas, OSINT y la

[566] *Jabber* es quizás menos conocida que otras herramientas de comunicación. Esta es una herramienta de comunicación integral para empresas, que permite utilizarla para enviar mensajes instantáneos, realizara llamadas telefónicas, unirse a teleconferencias y administrar contactos.

[567] *ICQ* es una aplicación de mensajería multiplataforma, de modo que se permite chatear con una misma cuenta en el móvil, web, Windows, Mac y Linux. A diferencia de Whatsapp, estas versiones funcionan de forma independiente, sin necesidad de mantener el móvil encendido y conectado.

presentación de solicitudes adicionales a operadores, a los segundos proveedores de correo electrónico y a los operadores de telefonía móvil. Esto puede continuar hasta que se agoten todas las opciones viables o se establezca la identidad del sospechoso.

Este proceso puede durar meses (incluso años), ya que muchos de los proveedores se encuentran en diferentes jurisdicciones. Además, el análisis forense tras el acceso al contenido del correo electrónico suele requerir mucho tiempo y recursos. Dependiendo del caso, los investigadores podrán vincular un nombre a una plataforma de comunicación en línea como Jabber, o a cualquier otra plataforma de comunicación, red de medios sociales o sistema de procesamiento de pagos. En este caso, se requiere la interceptación legal, así como un análisis más profundo (contenido, análisis de redes sociales, etcétera). Es probable que esto desencadene nuevas solicitudes e inicie ciclos de análisis adicionales hasta que se agoten todas las opciones o se establezca la identidad del sospechoso.

b) *Dirección IP*: si el punto de partida es una dirección IP, el investigador identifica el proveedor de servicios correspondiente y envía una solicitud para recibir la BSI. Esto se coteja y complementa con el análisis OSINT, y puede desencadenar solicitudes adicionales a los operadores. Este sería el escenario más fácil. Sin embargo, en la mayoría de los casos el proveedor del servicio utiliza tecnologías Carrier Grade NAT (CGN) para compartir una única dirección IP entre varios abonados. Se requiere entonces información adicional, como los números de puerto de origen, para que el operador pueda identificar a un abonado entre los posibles cientos o miles que utilizan la misma dirección IP en un momento determinado. Sin los números de puerto de origen, estos sólo pueden proporcionar una lista de suscriptores que luego deben ser investigados individualmente para posiblemente identificar al sospechoso. Los números de puerto de origen casi nunca son registrados por los proveedores de contenidos de Internet. En el caso de un proveedor de VPN, los investigadores sólo suelen recibir información sobre el pago (por ejemplo, datos de tarjetas de crédito,

criptomonedas u otro sistema de pago alternativo: PayPal, WebMoney, etcétera). Esto dará lugar de nuevo a nuevas solicitudes con el objetivo de identificar al sospechoso.

c) *Monedero de Bitcoin*: El proceso de análisis es similar al de los ejemplos anteriores. Los investigadores cotejarían el monedero de Bitcoin identificado durante la investigación con los datos de las operaciones existentes y también realizarán un análisis forense de *blockchain*. En un siguiente paso, el investigador intentará asociar el monedero a otros monederos potencialmente conocidos e idealmente rastreará la transacción financiera hasta un *cambiador*, donde el dinero virtual se convierte en moneda fiduciaria. Si este responde a la solicitud de las fuerzas de seguridad, puede que sólo tenga una dirección IP del cliente en el peor de los casos. Otros pueden tener los números de las cuentas bancarias u otra información personal identificable, dependiendo de la implementación/cumplimiento de las normas contra el blanqueo de dinero y del grado de conocimiento de su cliente. Seguirán otras solicitudes, también en diferentes jurisdicciones. Aparte de la complejidad técnica, es destacable el tiempo que llevará todo este proceso.

d) *Abuso y explotación sexual infantil en línea*: Los datos se cotejan con las bases de datos de información existentes y con el trabajo forense y analítico. Los problemas de conservación de datos se producen con regularidad, ya que los periodos de conservación de datos en los países suelen expirar entre la fecha del incidente inicialmente denunciado y la posterior fecha de difusión de la información. Esa gran cantidad de información que debían examinar los investigadores y el tiempo necesario para solicitar los datos a menudo hace que se pierdan posibilidades de investigación, incluso cuando la información se ha obtenido inmediatamente.

   En los casos más complejos se necesitan más recursos para realizar el trabajo analítico y enriquecer la información. Por ejemplo, en otro caso, el informe inicial contenía una dirección IP relacionada con un delincuente responsable de la posesión, fabricación y distribución de material de explotación sexual infantil en línea. El marcador de la dirección IP se remontaba a marzo de 2016. Cuando

se completó el trabajo de análisis era junio de 2016, lo que significó que los datos de los abonados de la dirección IP ya no podían solicitarse al proveedor de servicios de Internet de ese país y utilizarse como prueba contra el sospechoso.

e) B*ulling y otros comportamientos de abuso:* Se denunció a la policía la existencia de graves mensajes amenazantes contra una persona a lo largo de varios meses a través de las redes sociales. Estos mensajes también iban acompañados de otras pruebas, por ejemplo, daños contra la propiedad, pruebas de intentos de robo o de robos reales, regalos/mensajes dejados en el lugar de trabajo/domicilio que contenían amenazas, etcétera. Durante la investigación inicial, las pruebas físicas recuperadas no pudieron conducir a la identificación del individuo o individuos implicados. Se inició una investigación sobre con solicitud de información al proveedor de las redes sociales para recuperar un listado de direcciones IP asociadas al acceso a la cuenta en cuestión, que ya había sido cerrada. Sin embargo, el acceso se produjo en última instancia desde un dispositivo móvil para el que el proveedor de servicios no pudo vincular las direcciones IP a un usuario abonado específico debido al uso de CGN, cerrando así una posible línea de investigación para identificar a los sospechosos. Al final, los servicios policiales no pudieron utilizar los datos de comunicación como elementos de investigación para identificar a los sospechosos.

De estos ejemplos ficticios, pero equiparables perfectamente a otros reales y cotidianos, se observa que una clasificación de los datos por categorías, según su importancia, no es operativa, ya que la experiencia ha demostrado que las investigaciones comienzan con los datos disponibles para un delito concreto. Los datos en ese momento disponibles serán los considerados como más relevantes, y pueden diferir de un caso a otro. Como se observa en los ejemplos anteriores, puede ser una dirección IP, un número de teléfono, un apodo de un usuario en línea, una cuenta en una red social, un monedero de Bitcoin, etcétera.

Teniendo esto en cuenta, una opción más razonable podría ser aplicar diferentes criterios a las distintas categorías de datos en función del nivel de interferencia en los derechos de los afectados: sospechosos, víctimas y también de otras personas no implicadas en los hechos investigados, pero sí relacionadas de alguna forma. Este enfoque reflejaría también los distintos niveles de autorización necesarios, lo que, extrapolado a las investigaciones tradicionales, diferenciaría, por ejemplo, la actuación policial frente a la que requeriría de la autorización de un juez o un fiscal (según las diferentes tradiciones procesales de los Estados miembros).

1. El procedimiento legislativo ordinario en la Unión Europea

En el apartado anterior, hemos mencionado [ya lo habíamos hecho en numerosas ocasiones en los capítulos anteriores] a las distintas instituciones europeas; en este caso, respecto de los pronunciamientos que han ido haciendo como reacción a las sentencias del TJUE. Estamos entrelazando párrafos en los que se exponen los posicionamientos de la Comisión, del Parlamento Europeo y del Consejo de la Unión Europea [también hemos mencionado en otras ocasiones a agencias u organismos concretos que tienen un carácter consultivo o que, sin ser preceptivo su parecer, se les tiene en cuenta por la relevancia o especialización de sus criterios; no obstante, en este caso no los mencionaremos, salvo alguna referencia muy concreta]. Creemos que para entender adecuadamente cuál es el rol de cada uno de ellos a la hora de aprobar una norma europea y la interrelación entre ellos, es conveniente dedicar un apartado a explicar y profundizar en el proceso legislativo en la Unión Europea y, de forma particular, en el procedimiento legislativo ordinario [antes del Tratado de Lisboa, llamado de codecisión], puesto que es el que se siguió para aprobar la Directiva 2006/24/CE y, en consecuencia, las mismas instituciones que participaron en ese proceso están ahora llamadas, de una u otra forma, a ejercer el mismo rol; si se quiere, a encontrar una solución a nivel europeo, probablemente a través de una nueva directiva o reglamento que regule la conservación de datos de comunicaciones electrónicas.

En la Unión Europea, a diferencia de la práctica habitual en sus Estados miembros, [en los que la competencia para legislar reside en los parlamentos nacionales casi de forma exclusiva, al margen de determinados supuestos concretos y limitados en

los que se faculta a los gobiernos a actuar como legisladores, que después deben ser aprobados por esos mismos parlamentos], la competencia legislativa se ejerce por las tres instituciones principales: la Comisión, el Consejo y el Parlamento. Esta distribución competencial, que ha ido variando a lo largo del proceso de formación de la Unión Europea, es en ocasiones difícil de entender desde un punto de vista nacional y, además, complica enormemente el proceso de toma de decisiones y la negociación interinstitucional. No pretendemos hacer un repaso histórico de cómo hemos llegado a este sistema, por cuanto es simplemente tangencial al objeto de nuestro estudio. En el caso de la Directiva de Conservación de Datos, se aprobó con anterioridad al sistema de toma de decisiones introducido por el Tratado de Lisboa, y no se cuestionará si era el correcto; simplemente se analizará, para tratar de identificar sus debilidades y fortalezas e intentar ver si nos permite obtener alguna conclusión sobre la declaración de nulidad de la Directiva.

La Unión Europea ha evolucionado a lo largo del tiempo en cuanto a los mecanismos de producción normativa, concentrando y simplificando su número y dinámica, hasta que el Tratado de Lisboa los redujo principalmente a dos: el procedimiento ordinario y el procedimiento especial. Esta evolución también ha afectado a la participación y al peso de las distintas instituciones europeas con capacidad normativa; en la práctica, ha otorgado mayor peso al Parlamento Europeo. Con una mentalidad nacional nos produce sorpresa que no fuera así desde el principio, puesto que es la institución que recoge de forma directa la voluntad de los europeos, mediante su voto. Y es preciso mencionar otra característica distintiva de los parlamentos nacionales: la Unión no despliega esa capacidad ante cualquier materia, es decir, no tiene una capacidad legislativa general; se reduce a lo que recogen los Tratados y, para cada cuestión concreta que se aborde, tendrá que ser regulada por un instrumento legislativo específico entre aquellos con que cuenta la Unión Europea: reglamento o directiva, fundamentalmente, aunque para regular determinadas políticas se puede elegir entre ambos. Garzón Clariana (2015; 49)[568] se refiere a esta situación indicando que con anterioridad al Tratado de Maastricht, la participación de Parlamento Europeo en los procedimientos para la adopción de actos legislativos se ceñía

[568] GARZÓN CLARIANA, G., *"El Parlamento Europeo y la evolución del poder…"* op., cit., p. 49.

únicamente a la fase de preparación, mediante la emisión de informes no vinculantes y lo que en "la doctrina -inspirándose en una distinción clásica de Montesquieu- se ha dado en llamar el *'poder de impedir'*".

Puesto que pretendemos entender fundamentalmente la dinámica de la negociación interinstitucional y, en la mayoría de los casos es similar tanto si se trata de una directiva como de un reglamento (al margen de cuestiones muy concretas a las que nos referiremos de forma particular más adelante), nos centraremos en el procedimiento legislativo ordinario en general.

La propia denominación de este procedimiento indica que se puede considerar como el utilizado *"por defecto"*, de forma habitual y normal, es decir, es el procedimiento ordinario. Como venimos diciendo, antes del Tratado de Lisboa, se le denominaba de codecisión y estaba regulado por el artículo 251 del Tratado de la Comunidad Europea[569]. Ya en ese tiempo, la práctica y uso del procedimiento fue estableciendo un nivel de cooperación creciente entre ambas instituciones europeas, hasta el punto de que, según Capatorti (1986; 16) [570] se recurría cada vez menos al comité de conciliación previsto para los casos de desencuentro entre ambas instituciones europeas. Considera el mismo autor que el hecho de que se pusiera en plano de igualdad al Parlamento y al Consejo, otorgaba mayor legitimidad democrática al procedimiento, salvo cuestiones reseñables, pero de entidad menor, como el que el primero tuviera un plazo tasado para sustanciar el expediente y el Consejo no tuviera ninguna restricción temporal.

[569] En este procedimiento, la Comisión es quien presenta la propuesta normativa inicial y las otras dos instituciones, tras un procedimiento de negociación, la aprueban, en primera o segunda lectura, dependiendo de las dificultades que encuentren para alcanzar consenso sobre el texto trabajado. En ausencia de acuerdo, se debía recurrir a un comité de conciliación, en el que estaban representadas en plano de igualdad ambas instituciones, que debía proponer otro texto alternativo al Parlamento y al Consejo para su aprobación.

[570] CAPATORTI, F., *"El procedimiento de producción legislativa en las Comunidades Europeas"*, 1986, en *Revista Española de Derecho Constitucional*, pp. 260-262; y MANGAS MARTÍN, A., *La reforma institucional en el Tratado de Reforma*, en Revista de las Cortes Generales, 2007, p. 127-154.

Posteriormente, el Tratado de Lisboa recoge el procedimiento de codecisión y lo transforma en el conocido como procedimiento legislativo ordinario, regulado en los artículos 289.1 y 294 del TFUE. Mantiene la misma característica de generalidad en cuanto a su uso para la mayoría de los ámbitos cuya regulación corresponde a la Unión Europea. No es todavía el momento de particularizar para las materias correspondientes al ámbito penal, pero podemos adelantar que este procedimiento es también seguido de forma cotidiana para regular este tipo de políticas.

La iniciativa legislativa y, por tanto, la presentación de las propuestas, siguen correspondiendo a la Comisión Europea, como defensora y guardiana de los intereses comunitarios; sin embargo, en materia de derecho penal, esta competencia es compartida con los Estados miembros[571]. No es la única materia que no ha sido cedida plenamente por los países miembros a la Unión Europea, pero, tanto en este caso como en los otros [que no citaremos], indican el hecho de que no se ha avanzado tanto en integración como para que los estados cedan su capacidad punitiva en la institución comunitaria. Además, como salvaguarda, se establece también un mecanismo reforzado para evitar que un solo país pueda instar a la Comisión a presentar determinadas propuestas; en ese sentido, es necesario unir los intereses de un tercio de los Estados miembros a los de la Comisión si se quiere instar a presentar alguna iniciativa, consiguiendo así mayor legitimidad [esta prerrogativa que permite unir a varios miembros de la Unión Europea, nos da una idea que consideraremos al final de nuestra tesis, como opción para plantear alguna acción a nivel comunitario]. Existen otros mecanismos, como también lo podemos encontrar en España, como es la iniciativa popular. De todas formas, la Comisión busca legitimar sus propuestas en la mayoría de los casos mediante la inclusión del parecer de los grupos de interés afectados que, en cierto modo, trasladan los intereses de los ciudadanos, o al menos de una parte de ellos.

Es paradójico que la institución que nace de la soberanía popular no tenga capacidad de iniciativa legislativa como la que se otorga por los Tratados a la Comisión. De hecho, su papel en este sentido se limita a aprobar mociones instando a la Comisión a actuar ante determinada demanda o hecho concreto, de forma que es esta la que decide

[571] Según recoge el artículo 76 del TFUE.

atender o no la solicitud del Parlamento y en qué momento y, si no lo hace, basta con que explique los motivos. Incluso aunque no se niegue a atender la solicitud del Parlamento Europeo, puede transcurrir mucho tiempo entre el primer requerimiento y la actuación posterior de quien goza de la capacidad de presentar propuestas. Son muchos los casos en los que el Parlamento reitera su solicitud a la Comisión para actuar en un determinado asunto que considera prioritario para los intereses de los ciudadanos europeos. Es cierto que la discrecionalidad de la Comisión tiene ciertos límites, según prevé el artículo 265 del TFUE, ya que se habilita a esta institución a interponer un recurso ante el TJUE, por inacción ante la petición.

Desde el punto de vista formal, las propuestas que presenta la Comisión deben basarse siempre en alguno de los preceptos normativos recogidos en los Tratados, lo que se suele expresar como *base jurídica*[572]. Este aspecto es de suma importancia, pues, como hemos visto en el caso concreto objeto de nuestro estudio, la elección de unos u otros artículos de los Tratados como base jurídica y, por tanto, la incardinación en una u otra política europea concreta, puede tener consecuencias muy importantes[573]. Recordemos en ese sentido la primera iniciativa para regular la conservación de datos de las telecomunicaciones, que en 2004 se hizo bajo el paraguas del Tercer Pilar y no prosperó por discrepancias entre las instituciones europeas; o la propuesta de Directiva de 2006, que se amparó en el desarrollo del mercado interior y, a criterio de muchos expertos, fue uno de los motivos que dio lugar a la presentación de cuestiones prejudiciales ante el TJUE y a los pronunciamientos concretos de invalidez de esta norma europea.

Por otro lado, también debe respetar la Comisión los principios de proporcionalidad y subsidiariedad que se recogen en el artículo 5 del TUE, de forma que solo se regulará a través de una norma comunitaria en los casos en que los Estados miembros, de forma individual o entre varios de ellos, no puedan alcanzar los mismos objetivos de manera suficiente. Es decir, se considera que, incluso dentro del ámbito de

[572] En capítulos anteriores nos referimos a esta cuestión, al analizar la argumentación utilizada tanto en la propuesta de la Directiva 2006/24/CE como para las propuestas de interoperabilidad de las bases de datos y del sistema PNR.

[573] Según el artículo 5.1 del TUE, las competencias que tiene asignadas la UE se rigen por el principio de atribución.

competencias de la UE (para las compartidas), no siempre la Comisión puede presentar una propuesta normativa; en un segundo nivel de análisis se debe valorar de qué manera se es más eficaz [podríamos decir también eficiente] en la consecución de los objetivos propuestos con la política concreta de que se trate[574]. No volveremos a hablar del principio de proporcionalidad, que ya se trató de forma específica en su momento, si bien el mismo artículo del Tratado de la Unión Europea también se refiere a este como uno de los principios a seguir ante cualquier propuesta normativa de la Comisión, de forma que expresa la *obligación* de no excederse, con la medida de que se trate, de lo necesario para alcanzar los objetivos previstos. Este ha sido otro de los argumentos del Tribunal de Luxemburgo, el principal, para declarar la nulidad de la Directiva europea de conservación de datos de 2006.

Hay más principios y criterios que la Comisión debe tener en cuenta, y así los valora en sus propuestas normativas, pero reseñaremos solo uno más, que por obvio no debería ser necesario citarlo, si bien (aunque consideramos que no de forma intencionada) no siempre es tenido en cuenta y, en ocasiones, el Tribunal de Justicia tiene que recordarlo a través de sus sentencias, como ha ocurrido con la Directiva de 2006 invalidada. Nos referimos al respeto de los derechos fundamentales que recoge la Carta que, como ya dijimos, el Tratado de Lisboa incorporó como instrumento vinculante.

Otros organismos, que hemos venido citando a lo largo del estudio, tienen que ser consultados durante este proceso; otros no son preceptivos, pero también se incorporan sus opiniones a la evaluación de impacto. De hecho, algunos de estos organismos tienen una relevancia especial y, dependiendo de la materia concreta de que se trate, tienen un peso específico importante en la decisión de quienes deben trabajar la propuesta normativa de la Comisión. El Comité de las Regiones[575] y el Comité

[574] En los años de trabajo en el ámbito de las instituciones europeas (en el Consejo de la Unión Europea, defendiendo los intereses de España en materia de Interior), en cada una de las propuestas presentadas por la Comisión sobre las que se trabajó, había un apartado que justificaba la necesidad y la oportunidad para abordar la materia a nivel europeo, por considerar que no podía hacerse a nivel nacional o regional con el mismo nivel de eficacia.

[575] El Comité de las Regiones es un órgano consultivo que representa a los entes regionales y locales de Europa compuesto por representantes elegidos a escala local y regional, procedentes de todos los Estados miembros. A través de él, los representantes puedan dar a conocer su opinión sobre la

Económico y Social[576] deben ser consultados de forma preceptiva y, en función de la materia concreta, también puede ser necesario el dictamen del Tribunal de Cuentas, o el Banco Central o incluso el Tribunal de Justicia europeo. Existe otro tipo de actores con gran influencia a la hora de fijar la postura inicial de la Comisión, que se extiende a todo el proceso posterior de negociación: *los lobbies*. En el entorno físico de las instituciones europeas en Bruselas es frecuente ver carteles en edificios de organizaciones de todo tipo que representan a sectores empresariales e industriales que están en contacto permanente con todas las partes involucradas en el desarrollo de políticas europeas, y es constante la comunicación de estas organizaciones e individuos con los decisores políticos y técnicos para explicar sus postulados e intentar que las propuestas recojan sus intereses y los de las organizaciones y ciudadanos a los que representan.

Posteriormente, se inicia el proceso de deliberación de forma independiente y paralela por cada uno de los colegisladores, de acuerdo con lo recogido en el artículo 14.1 del TUE para el Parlamento Europeo y en el 16.1 para el Consejo; un proceso en el que cada uno de ellos actúa con un peso igual, lo que, como decíamos, no supone actuar en plano de igualdad entre la institución que representa a los ciudadanos y aquella que representa a los gobiernos de los Estados miembros. Aun así, se ha producido un cierto avance tras la aprobación del Tratado de Lisboa.

Nos detendremos en esta parte del procedimiento, al ser el más importante a nuestro juicio, dado que como decimos, de forma paralela ambas instituciones *trabajan* la propuesta inicial de la Comisión[577] y llegan a un nuevo texto que, por la experiencia propia, en muchas ocasiones difiere notablemente del esquema y concepto que la

---

legislación de la Unión que repercute directamente en las regiones y las ciudades, en https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cor_es

[576] El Comité Económico y Social es un órgano consultivo que representa a las organizaciones de trabajadores y empresario y otros grupos de interés y está compuesto por 329 miembros procedentes de los Estados miembros de la Unión. Emite dictámenes sobre cuestiones de la UE para la Comisión Europea, el Consejo de la UE y el Parlamento Europeo, y actúa como puente entre las instituciones de la Unión con capacidad decisoria y los ciudadanos europeos, en https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eesc_es

[577] Una propuesta normativa en la que el borrador de texto va acompañado de varias adendas que recogen una muy detallada evaluación de impacto en la que se incorporan exposiciones sobre cada uno de los aspectos recogidos, el aval jurídico de la propuesta, el cumplimiento de los principios que vimos antes (proporcionalidad, subsidiariedad, etcétera), la valoración económica de la puesta en práctica de la medida de que se trate, el parecer de las distintas partes interesadas, etcétera.

Comisión había elaborado sobre cómo abordar el problema concreto de que se trate. Cuando el Consejo y el Parlamento ponen en común sus textos y comienzan a negociar de forma conjunta, en lo que se conoce como *"trílogos"*[578] (teniendo en cuenta la distinta visión y enfoque que cada uno de ellos tiene sobre cómo abordar un problema, por su propia naturaleza y por la diferente visión sobre cómo defender los intereses de los ciudadanos o de los Estados), el punto de partida para obtener un texto común y consensuado no siempre es fácil. De hecho, en muchas ocasiones se alargan las negociaciones durante meses o incluso años, o concluye una determinada legislatura sin llegar a acuerdo (esto ocurre principalmente en expedientes sobre materias que tienen una alta carga política, ya que ante dosieres más técnicos suele ser más fácil alcanzar un acuerdo). Esta situación que describimos está basada en la práctica habitual, ya que podría no tener que alargarse el procedimiento en demasía si ambas instituciones llegaran a un acuerdo de forma rápida (como prevé el artículo 294 del Tratado de Funcionamiento de la UE) y la propuesta normativa se aprueba en primera lectura. Explicaremos a continuación esta afirmación con más detalle.

En una primera lectura, el Parlamento y el Consejo examinan la propuesta de la Comisión. En este momento inicial, el Parlamento puede aprobar la propuesta o rechazarla y, en el primero de los casos, puede hacerlo con enmiendas o sin ellas. El Consejo podría también aprobarla en su redacción inicial. En el mejor de los casos, en que ambas instituciones opten por la vía más rápida y favorable, se adoptaría el acto legislativo. Aun así, no están sujetos a plazos o tiempos para concluirla, lo que puede alargar la aprobación sin ni siquiera haber observado o manifestado problema alguno ni con el texto inicial ni en la forma de abordarlo por ambas instituciones. No defendemos que tenga que ser un procedimiento muy rápido, ni obviamos la carga de trabajo que se acumula y que obliga a atender a diferentes expedientes muy relevantes y de forma simultánea, pero el paso del tiempo hace que, en determinados asuntos en los que se ha planteado una necesidad urgente (muchos de ellos relacionados con el ámbito de la Seguridad) se pierda eficacia y, por qué no, también crédito de las instituciones europeas ante sus ciudadanos. Una vez más, consideramos que no es la práctica

[578] Se utiliza este término porque en él participa también la Comisión, aunque su función es apoyar el proceso de negociación del Consejo y del Parlamento y aclarar determinadas cuestiones que generen dudas o hacer alguna propuesta técnica sobre la redacción que van introduciendo y consensuando las otras instituciones europeas.

habitual, ya que se suelen presentar enmiendas y nuevas propuestas de redacción de numerosas partes tanto del articulado como del preámbulo. Respecto de la dirección de los trabajos, el Parlamento nombra a un ponente, que impulsará las fases del procedimiento y las negociaciones con las otras instituciones (si procede); el Consejo encargará los trabajos a la presidencia de turno, lo que puede derivar (como así ocurre) en que un mismo expediente pase por varias presidencias del Consejo de la Unión Europea[579].

En este punto, el devenir de la propuesta sigue caminos y circuitos diferentes en el Consejo y en el Parlamento. Aunque el objetivo final es el mismo: alcanzar un texto que satisfaga los intereses de la institución y de aquellos a quienes representan; la dinámica de trabajo está adaptada a la configuración y procedimientos propios de cada una de ellas.

En el caso del Parlamento, el ponente elabora un proyecto de informe de la comisión concreta a la que se ha asignado el dossier (en función de la atribución competencial de cada una de ellas)[580]. Aunque está asistido por expertos, él es quien introduce las primeras enmiendas al texto y decide si somete la propuesta a otros diputados u otras partes interesadas, para que contribuyan a este primer informe. Puesto que la Cámara europea está compuesta también por grupos políticos, cada uno de ellos nombra a sus ponentes alternativos para defender e introducir en el texto su posición política. Además, una vez presentado el proyecto de informe, según establece el artículo 218 del reglamento interno del Parlamento Europeo, cualquier diputado (siguiendo unas cuotas de representación mínimas) puede presentar también enmiendas, según un plazo concreto determinado por el ponente.

[579] Es muy importante el papel de la Secretaría General del Consejo que, como órgano permanente, asiste a las sucesivas presidencias y aporta el conocimiento práctico de la dinámica de las negociaciones y se constituye también en la "memoria histórica" del trabajo del Consejo. Esto implica una oportunidad y garantía de estabilidad en el ritmo de trabajo, pero también supone un riesgo, cual es el hecho de que, dependiendo de la actividad o liderazgo de la presidencia de turno, las negociaciones se encaminan hacia el criterio del Estado miembro que preside o de la Secretaría General del Consejo, que se constituye como un poder fáctico real.

[580] Para la Directiva 2006/24/CE de Conservación de Datos, como para la mayoría de los expedientes que afectan a materias de seguridad y de libertades, fue la Comisión LIBE la encargada de sustanciar esta propuesta de la Comisión.

Aquí observamos dos elementos interesantes sobre los que merece la pena hacer alguna consideración. Por un lado, la figura del ponente y su adscripción a un determinado grupo político del Parlamento, que tendrá consecuencias sobre el enfoque a dar a la propuesta, quizás influido también por la posición del partido político en su país de procedencia y que, en consecuencia, permitirá, por matizar determinadas enmiendas y la redacción de algunos puntos concretos de la propuesta y, por otro lado, fijar en el texto la posición de su país respecto de la medida concreta que se esté negociando. El otro elemento que queremos destacar es la dificultad que se introduce en el procedimiento, al permitir la presentación de enmiendas en diferentes momentos y tanto por quienes están realizando la ponencia, como por los miembros del comité encargado, o de cualquier diputado que reúna ciertos requisitos (no difícilmente alcanzables); esta complejidad no siempre supone un enriquecimiento del texto sino en ocasiones todo lo contrario: un enrevesamiento que obliga a reducir el nivel de detalle en favor del acuerdo y, en consecuencia, acaba regulando meras generalidades [por suerte no siempre es así].

Una vez presentadas las enmiendas, se debaten en la comisión formada al efecto, junto con el proyecto de informe, y se someten a votación que debe ser aprobada por mayoría simple. De la misma forma que indicaremos a continuación para el Consejo, en este proceso de debate en comisión estarán también presentes los representantes de la Comisión Europea que han trabajo la propuesta inicial, a los que se escuchará cuando haya alguna duda o ante los debates de las enmiendas presentadas. De la misma forma, aunque no con tanta presencia como la Comisión, el Consejo también puede asistir a algunos debates y, de esa forma, obtener una información valiosa que pueda orientar las negociaciones de los Estados miembros en el Consejo y así facilitar un futuro texto de consenso entre ambas instituciones. De forma sucesiva con este proceso, para asuntos de especial complejidad, pueden establecerse también conversaciones con las otras instituciones implicadas antes de someter el informe al pleno del Parlamento, aunque esta decisión requiere de una mayoría cualificada de los miembros de la comisión y de la aprobación en el pleno[581] y, en todo caso, será provisional y habrá de ser examinada tanto por la comisión como por el Pleno.

[581] Según recoge el artículo 71del reglamento interno.

Una vez que se ha adoptado el informe (normalmente con enmiendas) por la comisión designada al efecto, este ha de someterse a la aprobación del Pleno del Parlamento Europeo, que en la mayoría de los casos establece un debate de fondo[582] en el que se pueden volver a presentar enmiendas, en este caso adicionales. La propuesta queda aprobada si existe mayoría simple, ya sea con enmiendas adicionales o sin ellas; también puede rechazar la propuesta en su totalidad. En este último caso, si bien el Alto Tribunal no prevé explícitamente la posibilidad de rechazo en la primera lectura (sí es posible en la segunda), el propio Parlamento Europeo ha considerado que es posible y, de hecho, lo ha hecho en un par de casos de 2011[583] y 2015[584]. En este punto nos preguntamos si *¿podría haber hecho lo mismo en 2006 con la propuesta de Directiva de conservación de datos?* La siguiente fase dependerá de no solo del nivel de consenso alcanzado en esta institución, sino también de cómo hayan avanzado los trabajos y el acuerdo en el Consejo.

En el caso del Consejo, comienza también sus trabajos al recibir la propuesta de la Comisión, una vez publicada tras la aprobación por el Colegio de Comisarios. Aunque esta institución avanzara de forma más rápida que el Parlamento, no puede aprobar en primera lectura su texto hasta que lo haga también en primera lectura la Cámara europea. A efectos prácticos, entendemos que este hecho no supondría nada más que una llamada de atención implícita al otro colegislador para descargar sobre él la responsabilidad de no avanzar más rápido y aprobar una medida o política concreta que se entiende que beneficiará de una u otra forma y en mayor o menor medida a los ciudadanos europeos.

La dinámica de trabajo del Consejo comienza con la asignación de la propuesta de la Comisión a uno de los múltiples grupos de trabajo que reúnen a los expertos de los Estados miembros, dependiendo del reparto competencial que la Secretaría General del

[582] En ocasiones, antes del debate en Pleno, se envía el texto aprobado por la comisión al Consejo y a la Comisión para que indiquen su posición ante las enmiendas propuestas. De esta forma, el pleno puede debatir también sobre la viabilidad de que el proyecto avance de forma adecuada o presente obstáculos más o menos difíciles de sortear.

[583] Propuesta relativa a las estadísticas europeas sobre seguridad frente a la delincuencia, 2011/0146 (COD).

[584] Propuesta sobre la posibilidad de que los Estados miembros restrinjan o prohíban el uso de alimentos y piensos modificados genéticamente en su territorio, 2015/0093 (COD).

Consejo ha establecido[585]. Esta es la primera fase de análisis y se desarrolla a través de reuniones en grupo de trabajo a las que asisten los expertos en la materia de los distintos Estados miembros, asistidos por los consejeros de sus Representaciones Permanentes ante la Unión Europea, y que se pueden alargar durante varios meses (incluso cuando no es un texto no excesivamente problemático o sensible) puesto que hay que ir desmenuzando cada uno de los artículos y considerandos de la propuesta. En este momento, cada país (cada *capital*, como se suele denominar en el argot de las negociaciones comunitarias) muestra sus singularidades y hace propuestas concretas que muchas veces indican una vocación nacional más que europea; es decir, las propuestas de redacción suelen ir encaminadas a orientar la política concreta de que se trate hacia un sistema parecido al suyo propio[586] más que a mejorar el sistema europea incluso aunque esto implique hacer concesiones y cambiar las políticas concretas que cada Estado miembro ha venido aplicando hasta ese momento. En estos momentos se observa también claramente cómo muchos Estados miembros miran a aquellos países más fuertes en el ámbito europeo, para percibir por dónde pueden ir los puntos de discusión más delicados a los aspectos de más difícil aprobación.

Cuando los debates en los grupos avanzan y se van definiendo las posiciones comunes en los aspectos más relevantes de la propuesta, o también cuando algunas de las partes centrales de esta no encuentran puntos de encuentro, se suele enviar algún documento al respecto para debate entre los Embajadores Representantes Permanentes de los Estados miembros ante la Unión, con la idea de orientar al Consejo a un nivel menos técnico y más político. Estas discusiones entre embajadores tienen lugar en el COREPER[587], en muchas ocasiones en más de un momento de las negociaciones, y

[585] El número de grupos de trabajo y su denominación ha ido variando a lo largo del tiempo. En ocasiones se crean grupos nuevos, en otras se unen algunos bajo la misma u otra nueva denominación, etcétera. La última remodelación de grupos de trabajo la llevó a cabo el Consejo en 2020, bajo la filosofía de reducir grupos, cerrar aquellos que han perdido sus competencias e integrar los comunes o de materias afines. En definitiva, se ha racionalizado la configuración de grupos de trabajo de expertos para hacer más ágil el tratamiento de los expedientes y agrupar aquellos que están interrelacionados y para los que es conveniente juntar a los mismos expertos o a diferentes expertos, pero bajo una misma dirección a nivel de los Estados miembros.

[586] Es curioso observar cómo, en determinados expedientes, se observan claramente las posiciones afines entre países próximos geográficamente: nórdicos y centroeuropeos, sur de Europa o países del Este.

[587] Comité de Representantes Permanentes de los Gobiernos de los Estados miembros. Ocupa un lugar central en el sistema de toma de decisiones de la Unión Europea, coordina y prepara los trabajos de todas las sesiones del Consejo y trata de llegar a un acuerdo que posteriormente se somete al Consejo de ministros correspondientes, según la materia. El COREPER suele dividirse en dos partes: I y II,

tratan de desbloquear aspectos que los técnicos no han sido capaces. A este nivel, tiene menos influencia la posición de las *capitales* y más la del Consejero y los embajadores, que tienen una visión más global del sistema de negociación y de otros expedientes relacionados con aquel que se somete a su consideración en ese momento [esto no quiere decir que se abandonen las ideas fundamentales que cada Estado miembro ha considerado como elementos de negociación, pero sí que se apuesta más por encontrar el consenso y por establecer alianzas entre Estados miembros hacia una posición que, aunque no lo sea al 100%, pueda satisfacer los intereses de varios países hacia una solución europea.

En diferentes momentos de la negociación, con ocasión de las reuniones de ministros en Consejo (bien en Bruselas o en Luxemburgo) la Presidencia de turno suele presentar un documento analítico de aquellos aspectos fundamentales, tanto si han sido acordados como si están pendiente de un impulso y orientación política, para que los expertos puedan seguir trabajando; en ocasiones se hace a título informativo y para constancia de que los ministros han sido informados y en otras para debate de orientación. Es cierto que, puesto que los expedientes suelen abarcar más de una presidencia de turno de la UE, cada uno de los Estados miembros que durante un semestre están al mando del Consejo intentan avanzar en expedientes que los anteriores no han podido sustanciar o cerrar aquellos que están próximos al acuerdo, apuntándose así éxitos políticos que puedan ser recordados. Esta circunstancia añade presión en determinados momentos, dependiendo de la fuerza del país que por turno ejerza la presidencia o, en otras ocasiones, de la proximidad de las siguientes elecciones al Parlamento Europeo o de la constitución de una nueva Comisión Europea, bien por cerrar el ciclo con un éxito o por no dejar el expediente para un nuevo parlamento, que podría tener que revisar otra vez la propuesta y retrasar la aprobación de las medidas. No siempre se consigue, especialmente en asuntos como, por mencionar uno concreto, el Sistema Europeo Común de Asilo (SECA), que ha mostrado claramente desde el principio las diferencias entre grupos de países que hace inviable encontrar un acuerdo satisfactorio para todos.

---

dependiendo de la temática y, en la mayoría de los casos, a las deliberaciones del I suele asistir el REPER Adjunto y al II, que trata cuestiones *más políticas* asiste el REPER, en https://eur-lex-europa.eu/ES/legal-content/glossary/coreper.html

Cuando el texto está suficientemente consensuado a nivel del Consejo y la Presidencia considera que se ha alcanzado un acuerdo amplio sobre la mayoría de las cuestiones planteadas por los Estados miembros, se suele presentar de nuevo ante el COREPER para obtener lo que se denomina el *enfoque general* que, si bien no es una aprobación formal, porque esta deberá ser otorgada por el Consejo de ministros correspondiente, en la práctica lo es para los casos en los que no hay ninguna dificultad claramente expresada por ningún país y, de esa forma, la aprobación por los ministros lo será en los puntos sin discusión del orden del día. Esta es la situación ideal que busca cada presidencia de turno, aunque es frecuente que se introduzca en la agenda de los ministros como punto de discusión, bien por la importancia del expediente, por la sensibilidad de la materia regulada o porque sea necesario reconocer el esfuerzo realizado y el hecho de haber alcanzado el acuerdo[588]. La aprobación es por consenso, lo que supone que no es necesario que todos los Estados miembros tengan que estar de acuerdo, sino que, según un sistema de representación en función del número de habitantes de cada uno de los países que forman parte de la UE, haya mayoría simple[589]. Son escasas las ocasiones en las que se hace necesario utilizar la *calculadora de votos* europea, puesto que antes de llevar para debate lo que se conoce como *orientación general del Consejo*, la presidencia de turno y la propia Secretaría del Consejo se han asegurado de contar con los apoyos necesarios[590]. Considera Fernández Ogallar (2014; 138)[591] que el sistema general de mayorías favorece llegar a acuerdos y, en consecuencia, se ha optado por este sistema debido a un punto de vista pragmático y, extrapolada esta reflexión al ámbito del derecho penal, indica una apuesta por la eficacia frente a otras consideraciones.

[588] En determinadas ocasiones, no es infrecuente que algún Estado miembro que no está de acuerdo con el texto aprobado o con algún aspecto concreto, haga alguna declaración por escrito para su incorporación al expediente –también expresada de forma verbal por el ministro correspondiente- para que quede constancia de su oposición total o parcial.

[589] Algunos Estados miembros y los países asociados a Schengen no votan en determinadas materias concretas, normalmente relacionadas con cuestiones de desarrollo del acervo de Schengen.

[590] En el año 2016, ante la adopción de un informe de la Comisión en el que se proponían medidas para subsanar las graves deficiencias observadas en el control de las fronteras exteriores de Grecia, como consecuencia de la crisis migratoria en Siria, se produjeron momentos de tensión porque expiraba el tiempo para poder adoptar el informe y no había consenso, según el sistema de pesos específicos entre Estados. Finalmente, la negociación dio lugar a la aprobación del informe de la Comisión que obligaba al Consejo a proponer la adopción de medidas a Grecia, aunque se presentaron declaraciones de apoyo a Grecia por algunos países del sur de Europa.

[591] FERNÁNDEZ OGALLAR, N., *"El derecho penal armonizado…"*, op. cit., p. 138.

Llegados a este punto en el que cada institución ha realizado los trabajos internos, salvando las dificultades que cada uno de ellos puede encontrar en el camino recorrido (buscar el acuerdo entre diputados, en un caso, y entre los diferentes Estados miembros en el otro), se inicia la parte formal de puesta en común y de negociación hacia un texto común; es la llamada fase de *trílogos*[592] *o de negociación interinstitucional*, en la que las cartas se han puesto ya sobre la mesa, puesto que en las fases anteriores puede haber representantes de una institución durante las reuniones de la otra (si no en todos los casos, sí en aquellos en los que se traten cuestiones importantes que pueden mostrar alguna dificultad especial). En este proceso vuelve a ser clave también la participación de los representantes de la Comisión que redactaron la propuesta normativa y que, por tanto, tienen un conocimiento profundo del contexto general y de las particularidades de cada una de las medidas recogidas. Normalmente esta fase es más corta que la anterior y se suele llegar a acuerdo sobre un texto final aceptado o aceptable para el Parlamento Europeo y para el Consejo (aunque nunca es satisfactorio al 100%) y también para la Comisión Europea. En el caso contrario, existen mecanismos para avanzar hacia el consenso o incluso para retirar la propuesta (en este caso por parte de la Comisión).

Para el caso en que el Parlamento y el Consejo no logren llegar a un texto de compromiso sobre la adopción de la norma dada, se prevé un procedimiento de conciliación, con miembros de ambas instituciones, encargado de adoptar una decisión final en un plazo tasado de seis semanas, de forma que, en caso de desacuerdo persistente, el Consejo podrá adoptar por mayoría cualificada un texto que integre la posición inicialmente expresada por la Comisión y las enmiendas del Parlamento y será sometido a esta última institución, con la potestad para, si no está de acuerdo, rechazar el texto, si logra alcanzar mayoría absoluta de rechazo. En caso de aprobación por el Parlamento, el Consejo también deberá someterlo a ratificación definitiva por mayoría cualificada de sus miembros.

[592] En español es más correcto utilizar el término *"diálogo tripartito"*.

La Comisión, además del papel que juega en las deliberaciones, no es un simple convidado de piedra, ya que, de acuerdo con el artículo 293 del Tratado de Funcionamiento de la UE, podrá modificar su propuesta mientras no se haya pronunciado el Consejo; es decir, mientras no se haya adoptado el instrumento legislativo en debate. También los parlamentos nacionales participan desde el principio en este procedimiento, puesto que la propuesta de la Comisión es comunicada a cada uno de ellos (con un informe emitido desde la REPER, al menos en el caso de España) para que pueda ser evaluado si se cumple con el principio de subsidiariedad, al que ya nos hemos referido; en cierto modo, aunque los parlamentos nacionales evalúan solo determinados aspectos concretos de la propuesta, la aceptan o al menos conocen su contenido con mucha antelación al momento en el que tendrán que incorporar la norma europea a su ordenamiento jurídico. Aranda Álvarez (2013; 104)[593] profundiza en el conocido como mecanismo de *"alerta temprana"*, al referirse a las relaciones entre el Parlamento Europeo y los parlamentos nacionales, superando una fase anterior en la que únicamente había un intercambio de información sobre los trabajos que uno u otros realizaban a otra en la que tanto el Parlamento Europeo como el resto de órganos de la Unión Europea han de dar cuenta a los parlamentos nacionales de sus actos legislativos. Como asevera Fernández Ogallar (2104; 138)[594], si se da un porcentaje concreto de votos en contra superior *"a un tercio de los que cuenta cada parlamento, o a un cuarto en los supuestos de normas relativas a la cooperación policial y judicial, la propuesta deberá ser reconsiderada por los órganos comunitarios, a lo que se suma que cuando la Comisión decida seguir con la propuesta legislativa en cuestión y haya mayoría de parlamentos nacionales en contra, deberá motivar su decisión, tras lo cual el Parlamento Europeo y el Consejo podrán decidir no continuar con dicha propuesta"*.

No hemos relatado el procedimiento en el caso de tener que acudir a una segunda lectura, o incluso una tercera lectura, por cuanto no supone más que un indicador de falta de consenso y la necesidad de profundizar más en los puntos de encuentro para alcanzar un consenso.

[593] Para profundizar, vid. ARANDA ÁLVAREZ, E., "*La alerta temprana en el procedimiento legislativo de la Unión Europea. Una reflexión sobre su utilidad desde la reciente experiencia española"*, Revista de Derecho Comunitario Europeo, nº. 44, 2013, pp. 101-153, p. 104.

[594] FERNÁNDEZ OGALLAR, N., *"El derecho penal armonizado…"*, op. cit., p. 174.

Al concluir la negociación entre colegisladores, tras un proceso final de *refinado* desde el punto de vista de los juristas y los lingüistas del Consejo y del Parlamento, se aprueba el texto final, que será publicado en el Diario Oficial de la Unión Europea.

Algunas cifras aportadas por el Parlamento Europeo en su *"guía práctica del procedimiento legislativo ordinario"*[595] publicado en septiembre de 2020, puede dar una idea práctica de la importancia de este procedimiento legislativo (antes del Tratado de Lisboa, llamado de codecisión):

- Entre los años 2014 y 2019 (8ª legislatura), los colegisladores adoptaron 401 actos con arreglo a este procedimiento,
- Entre los ámbitos prioritarios, justicia y asuntos de interior ha sido de los primeros, lo que indica la importancia que la Unión Europea concede a las políticas en este ámbito,
- El 99% de los expedientes tramitados con arreglo a este procedimiento fueron aprobados en primera lectura o mediante un acuerdo rápido en segunda lectura, lo que indica la capacidad de acuerdo entre los colegisladores,
- En esta legislatura, por primera vez desde la introducción del procedimiento de codecisión, no hubo conciliaciones,
- La duración media del procedimiento para los actos adoptados en primera lectura fue ligeramente inferior a 18 meses y los adoptados mediante acuerdo rápido en segunda lectura duraron una media de 39 meses. Esto indica claramente el aumento considerable de tiempo que se consume si no se llega a consenso en la primera lectura, que ya de por sí requiere también de un plazo largo[596].

En la propuesta de la Comisión para una Directiva sobre conservación de datos, se siguió el procedimiento de codecisión que, en líneas generales, se puede considerar el predecesor del ordinario. Ya en aquel momento cabía la intervención de los actores

[595] "Guía práctica del procedimiento legislativo ordinario", manual sobre la labor del Parlamento Europeo como colegislador, septiembre de 2020, Bruselas, PE 640,179, en https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/handbook-on-the-ordinary-legislative-procedure

[596] En el caso del Consejo, 18 meses supone que 3 presidencias de turno del Consejo tendrán que manejar el expediente y, en cierto modo, implicarse en él con más o menos interés, dependiendo de diferentes condicionantes.

que hemos visto ahora y también se plantearon dudas tanto por el Parlamento, como por los órganos consultivos acerca de la falta de garantías suficientes para aprobar el texto con la redacción inicialmente propuesta por la Comisión y la modificada y consensuada por los Estados miembros. Aun así, se aprobó y, en cierto modo, todos los participantes tuvieron alguna responsabilidad en ello. Ahora, una vez que no se cuestiona que la Directiva es nula, creemos oportuno aprender de los errores del pasado y, dado que el procedimiento legislativo ordinario será el que deba seguirse ante una nueva propuesta para regular la conservación de los metadatos de las comunicaciones electrónicas a los efectos de la investigación y persecución de delitos graves, es conveniente conocer bien el papel de cada uno de los participantes en el procedimiento y los contrapesos que el TFUE establece, además del marco que el Tribunal de Justicia europeo ha dibujado sobre cuáles serán los límites que no se pueden traspasar. Esto será así, si se opta por una nueva norma jurídica europea, en forma de directiva o, por qué no, de reglamento. A propósito de esto último, trataremos a continuación los principales elementos de cada uno de estos instrumentos jurídicos y qué condicionantes ofrece la elección de uno u otro en una materia como la que estamos estudiando.

La Directiva tiene como principal característica que establece unos objetivos mínimos que los Estados miembros están obligados a cumplir, mediante el procedimiento de transposición de esta a sus normativas nacionales. Se deja al legislador nacional la potestad de fijar criterios más restrictivos, si así lo deciden, por lo que su objetivo es armonizar la normativa de la Unión Europea sin constreñir a los Estados miembros en cuanto a los medios para cumplir. Por tanto, su aplicación no es inmediata, pues el proceso de transposición requiere que los parlamentos nacionales aprueben una norma que recoja los preceptos de la Directiva europea[597]. Como contrapartida a la *flexibilidad* que ofrece este instrumento, se deja amplio margen de actuación a los países y pueden llegar a regular en exceso algunos aspectos que, quizás inicialmente se había pretendido hacer mediante la propuesta inicial de la Comisión, pero que hubo de rebajarse el nivel de ambición en aras del consenso. Ejemplos claros de lo que queremos expresar con esta afirmación lo hemos podido ver en el caso de la Directiva 2006/24/CE, por ejemplo, en el período de conservación de los datos, que varía entre 6 meses y 24 meses y ha propiciado que algunos Estados miembros hayan

[597] Según establece el artículo 288 del TFUE.

optado por el período inferior y otros por el superior; o con la definición de delito grave, etcétera.

Otra característica relevante de este instrumento legislativo es que, si bien los Estados miembros pueden decidir el tipo de norma nacional mediante el que cumplir con lo regulado en la norma europea, se debe garantizar que sea clara, de fácil comprensión y que cumpla con el marco establecido. En este sentido, Fernández Ogallar (2014; 160)[598], citando a Capotorti, hace referencia a una sentencia del TJUE, de 5 de mayo de 1980 en el *caso 102/79*, en la que se dispone que *"importa que todo el Estado miembro dé a las directivas una ejecución tal, que responda plenamente a las exigencias de claridad y certeza de las situaciones jurídicas queridas por tales directivas, en el mejor interés de los operadores económicos establecidos en los demás Estados miembros"*. Ya hemos tratado con profundidad el papel del Tribunal de Luxemburgo como garante de los derechos de los ciudadanos europeos y es pertinente recordarlo también en este momento puesto que, ante el incumplimiento de un Estado miembro con lo recogido en el entrecomillado anterior (igual que en otros supuestos), se puede instar al Alto Tribunal a pronunciarse en defensa de los afectados. Como ejemplo, sirva la potestad que tiene la Comisión Europea para hacer seguimiento del cumplimiento de los plazos establecidos para la incorporación al derecho nacional de las directivas (también de los reglamentos comunitarios). En el caso de incumplimiento sostenido en el tiempo y sin aportar causa justificada suficiente a criterio de la Comisión, esta puede presentar una demanda ante el Tribunal de Luxemburgo contra el país afectado[599], tras el correspondiente expediente de infracción, que puede finalizar con una condena al país incumplidor, que cada vez es más alta[600].

[598] FERNÁNDEZ OGALLAR, N., *"El derecho penal armonizado…"*, op. cit., p. 160.

[599] En el caso de España, se han producido condenas por no transposición a tiempo -con la extensión "de gracia" incluida- de determinadas Directivas, como, a modo de ejemplo: la Directiva sobre protección de datos personales en el marco de la prevención y detección de infracciones penales. Directiva (UE) 2016/680.

[600] En un principio, el TJUE imponía una condena a pagar una cantidad fija o una cuota diaria hasta que finalizara el procedimiento nacional de transposición. Últimamente, el Tribunal ha optado por imponer ambas: una multa inicial y otra diaria hasta que se comunique, mediante copia de la publicación en el diario oficial del país afectado, que se ha incorporado al derecho nacional la Directiva en cuestión -acompañando también una tabla comparativa que demuestre cada uno de los preceptos de la Directiva y su correspondiente regulación nacional.

Indica la misma autora[601] que el TJUE considera que en ciertas ocasiones una directiva puede tener efectos directos, como los que despliega (lo veremos a continuación) el reglamento.

Respecto del Reglamento, según recoge el artículo 288 del TFUE, tiene un alcance general y es obligatorio y directamente aplicable en cada uno de los Estados miembros. Una diferencia principal e importante con la directiva es que no se reserva los Estados miembros ningún margen de adaptación ni ampliación de lo regulado por este tipo de norma europea. En consecuencia, es ejecutivo y despliega sus efectos sin que se haya aprobado legislación alguna a nivel nacional, aunque es práctica habitual que aprueben normas de desarrollo y de detalle de lo contenido en el reglamento.

Estas características propias del reglamento hacen que sea menos frecuente, como indica para legislar en materias de derecho penal, pues impondría obligaciones a los Estados miembros en una materia compartida sin otorgarles la capacidad de adaptación a su legislación nacional, sin que ello impida que la legislación de ejecución del reglamento pueda regular aspectos de índole penal.

2. Evolución del proceso de reflexión en el seno del Consejo de la Unión Europea

El punto de partida para un nuevo régimen de conservación de datos deberá atender a los requerimientos del TJUE y, en consecuencia, deberá definir los delitos y las circunstancias específicas para los que se podrán conservar los datos; los tipos de datos que puedan ser conservados; las medidas técnicas, de seguridad y organizativas para el acceso a los datos retenidos y las autoridades que puedan hacerlo; el sistema de autorización y de control que corresponderá a jueces y otras autoridades administrativas con competencia en la materia; procedimientos concretos para realizar la trazabilidad de los accesos; la duración de la conservación en función de los datos concretos y de la gravedad de los delitos para cuya investigación, persecución y enjuiciamiento sobre

[601] FERNÁNDEZ OGALLAR, N., *"El derecho penal armonizado…"*, op. cit., p. 161.

tratados. Aunque no es objeto de esta investigación, también será importante considerar los procedimientos y mecanismos para la transferencia internacional de esos datos.

Tras los primeros debates de 2017, los trabajos se centraron en tres elementos principales de un régimen de conservación a los efectos estudiados, sin excluir ningún otro posible elemento que pudiera surgir posteriormente:

- Garantizar la disponibilidad de los datos: en este sentido se consideró necesario mantener la coherencia entre el proyecto de Reglamento sobre la privacidad y las comunicaciones electrónicas y el régimen de conservación de los datos a efectos de prevención y enjuiciamiento de delitos. En primer lugar y como prioridad, las normas y obligaciones aplicables a los prestadores de servicios en el contexto del proyecto de reglamento no deberían impedir la posibilidad de adoptar normas específicas en la legislación nacional o de la UE, con la finalidad de conservar datos para la prevención y persecución de delitos. En este sentido, debería prestarse especial atención a una mejor delimitación del ámbito de aplicación del proyecto de reglamento a la vista de los argumentos del Tribunal derivados de la interpretación del ámbito de aplicación y de la estructura de la actual Directiva sobre la privacidad y las comunicaciones electrónicas. En este mismo sentido, cabe destacar que, en sus Conclusiones de 19 de octubre de 2017[602], el Consejo Europeo destacó *"la necesidad de una mayor transparencia en las prácticas y los usos de las plataformas"*.

- Restringir el ámbito de aplicación del marco de conservación a estos efectos, teniendo en cuenta las exigencias de la jurisprudencia.

- Establecer salvaguardias sólidas en relación con el acceso a los datos conservados basándose en una prueba estricta de necesidad y proporcionalidad.

De los debates celebrados entre expertos, se llegó a un consenso sobre la toma en consideración de un cierto número de principios y elementos específicos sobre los

[602] Documento EUCO 14/17.

que fundamentar la conservación restringida de los datos y el acceso selectivo a estos, en base a los pronunciamientos que el TJUE venía reiterando:

- La Carta *"no excluye limitaciones al ejercicio de los derechos y libertades"* contemplados en la misma, siempre que dichas limitaciones cumplan las condiciones específicas establecidas en el artículo 52, apartado 1 y, en particular, siempre que superen una prueba estricta de proporcionalidad y necesidad[603]. En lo que respecta a las categorías de datos, medios de comunicación, personas afectadas y periodo de conservación, debe establecerse una conexión entre los datos conservados y el fin perseguido sobre la base de criterios objetivos[604].

- La Carta *"no se opone"*[605] a la legislación sobre conservación de datos, pero el Tribunal excluye *"la conservación generalizada e indiscriminada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica"*. Sin embargo, no solo permite la conservación selectiva de datos.

- La medida debe limitarse a lo estrictamente necesario, basarse en pruebas objetivas y establecer normas claras y precisas. El Tribunal menciona que dicha limitación puede alcanzarse restringiendo la conservación a: i) datos pertenecientes a un determinado período temporal y/o a una zona geográfica y/o a un grupo de personas que pudieran estar relacionados de un modo u otro con un delito grave, o ii) personas que, por otros motivos, podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia[606].

- El ámbito de aplicación potencial de un sistema de conservación restringido de datos debe ser eficaz para la protección del interés de seguridad pública, de manera

[603] Se recuerda que, de acuerdo con la jurisprudencia reiterada, una prueba estricta de necesidad implica que no puede existir una medida menos intrusiva igualmente eficaz para alcanzar el objetivo perseguido.

[604] Sentencia TJUE, de 21 de diciembre de 2016, caso Tele 2 Sverige, apartado 110 y, más recientemente, PNR Canadá, apartado 191.

[605] Sentencia TJUE, de 21 de diciembre de 2016, caso Tele 2 Sverige, apartado 108.

[606] Sentencia TJUE, de 21 de diciembre de 2016, caso Tele 2 Sverige, apartado 106.

que las restricciones aplicadas no hagan que la medida deje de ser pertinente para los fines perseguidos.

- Unas salvaguardias y limitaciones sólidas en lo que respecta al acceso y uso por las autoridades competentes de los datos conservados contribuyen a mitigar los efectos generales de la interferencia de la medida, en particular velando porque el acceso se otorgue solo para los datos específicos necesarios para una investigación en particular, lo que debería reducir al mínimo los efectos sobre los derechos y las libertades individuales.

- Puede estudiarse un planteamiento diferenciado en lo que respecta a dos niveles de interferencia: *"de primer y de segundo nivel"*, teniendo como objetivo al mismo tiempo un marco de salvaguardias general compatible con las exigencias del Tribunal como resultado del efecto acumulativo de las salvaguardias específicas introducidas en cada uno de estos niveles, y cumpliendo ambos con los criterios de necesidad y proporcionalidad[607]:

a) Interferencia de nivel 1: *conservación restringida de datos*

Se acordó limitar las categorías de datos, retirando aquellos que se consideraran superfluos o que no sean necesarios a la vista de la experiencia acumulada, no centrando la justificación de los necesarios en grupos de personas o áreas geográficas específicas en el territorio de un Estado miembro, sin perjuicio de las prácticas nacionales en lo que respecta a la supervisión de grupos de personas en el contexto de procesos penales. Para materializarlo, se acordó desarrollar una matriz con diferentes categorías de datos *conservables* a efectos de investigación penal, excluyendo aquellas que no sean absolutamente esenciales[608].

[607] La conservación selectiva y el acceso limitado se entienden como condiciones cumulativas, de modo que el hecho de cumplir una no puede ser suficiente. En consecuencia, aun cuando no hay acceso sin conservación previa, cada una de las injerencias debe justificarse por separado, mediante un examen específico del objetivo perseguido y el cumplimiento con el principio de proporcionalidad respecto de la gravedad de la injerencia en los derechos afectados.

[608] No se ha podido tener acceso a la matriz resultante del estudio, ni siquiera se ha podido confirmar si está ya finalizada, por el carácter restringido que se le ha otorgado por parte de los expertos.

Esta matriz, a modo de ejemplo [no exhaustiva y de elaboración propia, basada en los documentos consultados y en la experiencia propia], debería contener los siguientes,[609] esenciales para el desarrollo de investigaciones complejas como las que se han relatado en los párrafos precedentes[610]:

Información básica del abonado

- Nombre/apellido

- Dirección

- Fecha de nacimiento

- Documento de identidad

- Dirección de correo electrónico

- Nombre de usuario

- Claves de la contraseña

- Número de teléfono

- IMSI - Identidad Internacional de Abonado Móvil

- IMEI - Identidad Internacional de Equipo Móvil

- Dirección IP en el momento del registro

- Fecha y hora de registro

- Puerto de origen en el momento del registro

- Dirección MAC en el momento de la inscripción

- Registros de información financiera (cuenta bancaria, número de tarjeta de crédito, etc.)

- Lista de contactos

- Contenido y hora de las actualizaciones de la información del abonado

[609] No prejuzga las diferentes experiencias en investigación de los Estados miembros de la Unión Europea u otros terceros países.

[610] Como se indicaba, dependiendo del caso concreto, el punto de partida de la investigación puede ser cualquiera de estas categorías de datos o una combinación de ellas.

Información sobre el tráfico

- Direcciones IP de conexiones recientes

- Hora/fecha, ubicación

- Identificador de la estación base

- Registros de la estación base

- BTS - Estación base de transmisión

- Volumen de tráfico

- Puertos de origen

- Dirección IP de destino

- Números de teléfono de origen/destino, incluido el número de teléfono, IMEI, IMSI, ubicación de la contraparte.

- Registros de conexión (incluyendo IPs, direcciones MAC, otros identificadores de máquinas/navegadores)

- Información de la empresa

- Información financiera (por ejemplo, historial de pagos)

- Actualizaciones de saldo de prepago

- Tiques

- Facturas

En relación con lo anterior, ya entonces existía un acuerdo común -tal como se mencionó en el Consejo JAI de junio de 2017- entre las delegaciones de los Estados miembros acerca de que la información básica de los abonados, en particular una dirección IP atribuida a un usuario, no pertenece al ámbito de aplicación al *Caso Tele2 Sverige*[611].

[611] Documento 9802/17 de la Secretaría General del Consejo.

Se acordó también explorar la posibilidad de remitir órdenes de conservación renovables dirigidas a los proveedores que operan en el territorio del Estado miembro sobre la base de una prueba de necesidad estricta realizada en relación con los distintos tipos de proveedores que ofrecen servicios: en función de su tamaño y del tipo de servicio y de las evaluaciones periódicas de las amenazas en cada Estado miembro por separado. Esta medida podría garantizar que la relación entre los datos conservados y el objetivo perseguido se determine en cada Estado miembro y se adapte a sus características específicas.

Respecto del período de almacenamiento limitado, se alcanzó consenso respecto de que no debería exceder de lo estrictamente necesario para los fines de la prevención y enjuiciamiento de delitos. Con objeto de seguir respondiendo al requisito del principio de proporcionalidad, podrían determinarse diferentes periodos de conservación en las distintas categorías de datos en función de su sensibilidad y exigirse la supresión irreversible de los datos al término del periodo de conservación, a menos que se conserven con fines empresariales.

Por último, sobre la seguridad de los datos almacenados, el Tribunal de Justicia requiere que se *"establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a los riesgos de abuso"*[612]. Por consiguiente, se valoró de forma positiva contemplar la posibilidad de prever requisitos para la seguridad de los datos, como el almacenamiento de estos en el ámbito territorial de la Unión Europea[613].

b) Interferencia de nivel 2: *acceso selectivo a los datos conservados*

Los criterios del Tribunal para el acceso a los datos almacenados y su uso se describen con claridad en los Casos *Digital Rights y Tele 2 Sverige*. A este respecto, se acordó tomar en consideración los siguientes elementos:

[612] Sentencia TJUE, de 21 de diciembre de 2016, caso Tele 2 Sverige, apartado 109.
[613] Sentencia TJUE, de 21 de diciembre de 2016, caso Tele 2 Sverige, apartado 122.

- Restringir el acceso con el fin de combatir solo determinadas categorías de delitos, como la delincuencia organizada, el terrorismo, el maltrato infantil, u otros delitos graves -por citar solo algunos- en la medida en que supongan un riesgo para la vida o una situación de urgencia en un caso concreto; o cuando puedan afectar gravemente la integridad física o psicológica de la víctima (por ejemplo, el acoso en línea); o en los casos de personas desaparecidas o de delitos favorecidos por el ámbito cibernético.

- Establecer normas claras y precisas que indiquen en qué circunstancias y en qué condiciones se podrá conceder acceso a los datos a las autoridades nacionales competentes, incluidos los requisitos materiales y procedimentales a tal efecto: i) *"… en principio solo podrá concederse un acceso…. a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave… No obstante, en situaciones particulares, como aquellas en las que intereses vitales para la seguridad nacional, la defensa o la seguridad pública están amenazados por actividades terroristas, podría igualmente concederse el acceso a los datos de otras personas cuando existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra dichas actividades"*[614]; ii) el acceso debe estar supeditado a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente (salvo en caso de urgencia); iii) pueden tenerse en cuenta exenciones para el acceso a datos de ciertas categorías de personas, por ejemplo, personas sujetas al secreto profesional; y iv) se deberá llevar a cabo la notificación a la persona de que se trate, siempre que no haya riesgo para los intereses de las investigaciones.

Las sentencias posteriores han ido aportando nuevos elementos de interés que permiten matizar estas posiciones iniciales, pero que no han podido ser valoradas en toda su extensión por los expertos que se reúnen en el ámbito del Consejo de la Unión Europea, porque los trabajos han quedado prácticamente parados, precisamente a la espera de esos nuevos pronunciamientos del Tribunal (que ya se han producido; alguno de ellos muy recientemente, como hemos tenido ocasión de exponer en este estudio). En

[614] Sentencia TJUE, de 21 de diciembre de 2016, caso Tele 2 Sverige, apartado 119.

consecuencia, cuando se retomen las discusiones sobre esta materia, estos criterios iniciales se mantendrán, pero habrá que modular alguno de ellos.

3. La aplicación de la ley en los Estados miembros ante la nueva situación

Ante la difícil situación creada a raíz de la invalidación de la Directiva, la Comisión, como complemento y apoyo a las discusiones que el Consejo había iniciado [quizás demasiado tarde, puesto que se esperó hasta la segunda sentencia (la de 2016) para comenzar un proceso serio de reflexión], presentó un concurso para que una consultora realizara un estudio detallado del impacto de la nueva situación en la actuación y labor diaria de los servicios policiales y en el proceso penal.

Aunque contó con algunas importantes limitaciones[615], permitió poner de manifiesto algunas cuestiones relevantes, tanto a favor como en contra de nuestros pensamientos iniciales y también de los expertos que llevaban ya tiempo discutiendo y valorando opciones para encontrar una solución adecuada. Por lo tanto, consideramos importante dedicar un epígrafe a resaltar los elementos más ilustrativos, a los efectos de nuestra investigación, porque pensamos que nos aportarán una imagen bastante completa de la medida en que la situación es más o menos grave, de la mayor o menor urgencia en la búsqueda de una solución de consenso y de si el impacto ha sido homogéneo o desigual en los países participantes. En ese sentido, del estudio se pueden extraer las siguientes conclusiones:

a) Respecto del *marco normativo e institucional* para la conservación de datos en los 10 Estados miembros incluidos en el estudio, se considera fragmentado: unos no tienen actualmente la obligación legal de que los proveedores de servicios conserven los datos que no son de contenido, para fines policiales; otros siguen aplicando (en líneas generales) la legislación nacional de transposición de la

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

Directiva (entre ellos está España); otros que no disponen de regímenes obligatorios de conservación de datos, los servicios policiales dependen de los datos de tráfico y de localización que conservan los proveedores de servicios electrónicos para sus propios fines comerciales o empresariales (no se exige la conservación a los operadores otros datos adicionales).

Existen pocas alternativas a la retención obligatoria de datos. La principal solución alternativa de que disponen las fuerzas de seguridad es una solicitud de conservación rápida de datos [*quick freeze*, como la hemos denominado en otras ocasiones anteriores], generalmente ordenada por la policía o la Fiscalía y que requiere una autorización judicial para obtener los datos. Sin embargo, sólo seis Estados miembros incluidos en el estudio han ampliado el mecanismo de conservación de datos más allá de la gama de ciberdelitos definidos por el Convenio de Budapest sobre la Ciberdelincuencia. Como la congelación rápida se refiere a los datos pasados que actualmente almacena el proveedor de servicios, su éxito depende a menudo de que los estos conserven incluso los datos que no son de contenido. En ese sentido, los participantes revelaron que no consideran esta opción como una alternativa adecuada y eficaz a la conservación general y obligatoria de datos que el Tribunal de Luxemburgo proscribe.

La situación creada por las sentencias del Tribunal llevó a una mayoría de los países consultados a cuestionar la validez de sus normas nacionales y, también la mayoría de estos, iniciaron procedimientos jurídicos o políticos en relación con sus marcos de conservación de datos; algunos incluso plantearon cuestiones prejudiciales ante el Alto Tribunal[616]. En consecuencia, se evidencia que esta inseguridad jurídica en relación con el marco legal sobre la conservación de datos y el acceso a los mismos es un reto primordial tanto para las agencias de seguridad como para los proveedores de servicios electrónicos en casi todos los Estados miembros. Incluso en los casos en los que las leyes nacionales sobre la conservación de datos siguen siendo válidas, el temor a que se anulen las

[616] Algunas de ellas ya han sido contestadas recientemente por el TJUE, por lo que han dado respuesta a las inquietudes de los países que acudieron a la instancia europea. Todos esos pronunciamientos han sido incorporados (y analizados) al presente estudio.

condenas debido a la inadmisibilidad de los datos de tráfico y localización en los procedimientos penales puede impedir que las fuerzas de seguridad soliciten el acceso a ellos (como así se manifestó en respuesta a la correspondiente pregunta del estudio).

En la mayoría de los países participantes se permite el acceso a los datos sin contenido por parte de los servicios policiales (en ocasiones, incluso a la policía militar) y las autoridades judiciales, así como a los servicios de inteligencia. Otros Estados miembros han ampliado el derecho de acceso a autoridades con competencia en materia fiscal, aduanera o en el ámbito de la competencia. Aunque estas autoridades no se consideran agencias encargadas de la aplicación de la ley en sí mismas, los datos no relacionados con el contenido sólo pueden solicitarse con fines policiales, por lo que la ampliación a otros servicios no policiales dificulta aún más llegar a una solución satisfactoria con los criterios marcados por el Tribunal.

En todos los países participantes, las competencias en materia de supervisión de las normas de conservación de datos se comparten entre los reguladores de las telecomunicaciones y las agencias de protección de datos. Aunque este solapamiento de competencias podría plantear problemas, no se observó ningún problema importante. Mientras que las segundas son las principales responsables de garantizar que los datos personales se traten de acuerdo con las normas y salvaguardias pertinentes, los reguladores de las telecomunicaciones son responsables de la supervisión de las obligaciones de los proveedores de servicios, en virtud de las leyes nacionales de conservación de datos[617].

b) Respecto de las *prácticas de conservación de los datos*, en general, los tipos de datos incluidos en la obligación de conservación son prácticamente los mismos en todos los Estados miembros con leyes de conservación de datos. Además,

[617] Esto es así, lógicamente, en el caso de los países en los que siguen vigentes las normas nacionales de conservación de datos.

todos los proveedores consultados conservan todos los tipos de datos que no son de contenido para al menos un fin interno (por ejemplo, negocio, comercial, facturación, marketing, seguridad de la red). Sin embargo, difieren a la hora de determinar aquellos datos que forman parte de estas categorías y el tiempo que los conservan.

Como hemos venido relatando, sobre la base del análisis de los marcos nacionales, los datos no relacionados con el contenido pueden clasificarse en tres grupos: datos de abonados, de tráfico y de localización. Esta clasificación es importante ya que, en algunos Estados miembros, las condiciones de acceso varían en función del tipo de datos solicitados. Existe un amplio consenso entre los participantes en el estudio acerca de la incardinación de los datos en cada uno de los grupos, con la excepción de algunos datos concretos: la dirección IP, el número de puerto para las direcciones IP dinámicas y los números de identificación del módulo de identificación del abonado (SIM) y del dispositivo (por ejemplo, la identidad internacional del abonado móvil (IMSI) o la identidad internacional del equipo móvil (IMEI)). Algunos Estados miembros consideran que estos datos son englobados dentro de los correspondientes a los abonados, mientras que otros los tratan como datos de tráfico.

c) El *periodo de conservación de datos* obligatorio para fines policiales es de 12 meses, excepto en dos países concretos en los que se establecen 12 meses para los datos de Internet y 24 meses para los datos telefónicos; y otro Estado miembro en el que se fijan 72 meses. Sin embargo, los periodos de conservación para los datos retenidos con fines comerciales no están claros: algunos Estados miembros establecen un periodo máximo de conservación de seis meses para los datos empresariales, mientras que otros utilizan un año. Dentro de estos límites, los periodos varían de un operador a otro, en función de sus normas internas. Los datos conservados a efectos de facturación suelen tener períodos de conservación más claros y largos, debido a los umbrales legales de impugnación de facturas[618]. Esto significa que, para las agencias encargadas de la aplicación

[618] Una media de tres meses.

de la ley, los datos más fiables disponibles en los registros internos de los operadores son los conservados a efectos de facturación. Los datos de los abonados suelen conservarse durante todo el tiempo que dura el contrato entre los clientes y el operador[619]; normalmente, varios años. La mayoría de los proveedores de servicios consultados por los redactores del informe manifestaron que conservan los datos de tráfico a efectos de facturación. Por el contrario, los datos de identificación y localización tienen un valor comercial limitado y se conservan durante periodos de tiempo mucho más cortos (incluso un período de 7 días, lo que los hace prácticamente inviables a los efectos de una investigación que necesite un histórico de datos un mínimo tiempo atrás)[620].

d) Las *direcciones IP*, en particular las direcciones IP dinámicas asignadas a varios usuarios a la vez a través de Carrier Grade (CG) NAT, destacan como el tipo de datos más difícil de obtener para las fuerzas de seguridad. Los números de puerto no se conservan en muchos de los Estados miembros e, incluso cuando se conservan, los investigadores necesitan precisar mucho el momento sobre el que necesitan la información para que los proveedores puedan identificar al usuario que está detrás de una determinada conexión.

e) Los *requisitos de seguridad* para el almacenamiento de datos son en general los mismos en todos los Estados miembros, ya que están relacionados con los estipulados en el Reglamento General de Protección de Datos y siguen siendo tecnológicamente neutros. Aun así, hay diferencias en el sentido de que algunos exigen que el almacenamiento se haga de forma separada de los que afectan a fines comerciales y de negocio. Por lo que se refiere a lugar de almacenamiento unos posibilitan su custodia en cualquier parte de la Unión Europea, mientras que otros deben hacerlo en territorio nacional.

[619] Estos datos son necesarios para la suscripción, por lo que deben mantenerse mientras esté vigente.

[620] Esta situación puede darse con mucha frecuencia, simplemente por el tiempo que pase desde que la víctima conoce la comisión de un delito, acude a denunciar el hecho ante la policía y se pone en conocimiento del juez, solicitando el acceso a los datos de los proveedores de servicios de telecomunicaciones.

f) Sobre el *acceso a los datos conservados*, a falta de obligaciones generales de información o transparencia para los Estados miembros o los proveedores de servicios, las estadísticas a las que tuvieron acceso en el estudio fueron muy limitadas y los participantes fueron reacios a compartir datos, dado lo delicado del asunto, por lo que no se pudieron extraer conclusiones respecto de la frecuencia de las solicitudes efectuadas. En los casos en los que se dispuso de estadísticas, se observó que hay una gran variedad de metodologías utilizadas para registrar y contabilizar las solicitudes que impedían poder efectuar comparaciones adecuadas entre países.

Sin embargo, de los datos aportados por los servicios policiales, se pudo confirmar la importancia de esta información para las investigaciones, pues más del 50% de los encuestados afirmaron haber solicitado datos en al menos el 60% de las investigaciones de los dos años anteriores al estudio[621]. Lo más habitual es que las solicitudes se refieran un individuo o dispositivo específico, siendo menos frecuente las solicitudes más indiscriminadas para obtener los datos de conexión, por ejemplo, a una torre de telefonía.

Las solicitudes de las fuerzas de seguridad incluyen todo tipo de datos de identificación, localización y tráfico, aunque los más frecuentes son el número de teléfono, la dirección física, la fecha y la hora de la comunicación y la ubicación del equipo o la línea al inicio de la comunicación. Por lo general, se solicitan datos en numerosas ocasiones en el marco de una investigación[622], aunque algunos datos se solicitan con mayor frecuencia para determinados tipos de delitos[623].

[621] 2018 y 2019. Años anteriores a la pandemia del COVID-19 y, por tanto, no afectados por la bajada tanto en la comisión de determinados delitos ni por la menor capacidad de investigación que se produjo por las medidas para hacer frente a la situación sanitaria mundial.

[622] Por ejemplo, registros de llamadas de un sospechoso que contienen fechas, horas y ubicación de las comunicaciones, así como los números a los que se llamó.

[623] Por ejemplo, las direcciones IP se solicitan con mucha más frecuencia para la investigación de fraude en línea, la ciberdelincuencia, la explotación sexual de los niños y otros delitos relacionados con la informática.

Las solicitudes de datos normalmente producen una respuesta positiva. La mayoría de los encuestados, tanto de los servicios policiales como los proveedores de servicios, afirmaron que las solicitudes no tienen éxito en menos del 20% de los casos. La razón más frecuente de contestaciones infructuosas es que los datos ya no se conservan en el momento de la solicitud.

La falta de estadísticas detalladas dificulta también analizar la antigüedad media de la información solicitada. En algunos Estados miembros que sí aportaron estadísticas, se observa que la mayoría de los datos solicitados tienen menos de seis meses de antigüedad. Sin embargo, el tipo de delito investigado desempeña también un papel importante en la antigüedad media de los datos necesarios, puesto que unos delitos se conocen en un breve espacio de tiempo, pero otros (especialmente los cometidos por medios electrónicos), pueden ser descubiertos bastante más tarde y, en consecuencia, se hace imprescindible acceder a datos más antiguos.

También hay diferencia respecto del tipo de delito para el que se solicita el acceso a los datos. En unos Estados miembros, de acuerdo con sus normativas nacionales, se restringe a determinadas categorías, mientras que en otros se pueden solicitar para cualquier tipo de ilícito penal. Sin embargo, el estudio indica que los investigadores ponderan la necesidad de los datos y la proporcionalidad de la medida y, en la práctica, sólo efectúan solicitudes cuando los consideran absolutamente necesarios, teniendo en cuenta la gravedad del delito y la disponibilidad de pruebas alternativas.

Por otro lado, la medida en que los metadatos son elementos de prueba decisivos en una investigación o a los efectos de enjuiciamiento en un proceso penal varía según el tipo de delito y el tipo de agencia encargada de la aplicación de la ley de que se trate; son, por ejemplo, de especial importancia en la investigación y el enjuiciamiento de la ciberdelincuencia, la explotación sexual infantil y la pornografía infantil; delitos suficientemente graves y rechazables por cualquier

ciudadano como para mostrar la importancia de contar con estos datos para garantizar la seguridad y pacífica convivencia de los ciudadanos. Esta información es a menudo el medio principal para detectar el delito y se convierte en un elemento clave. También pueden ser valiosos para las investigaciones y los procesos judiciales, incluso cuando no se utilizan como prueba principal. En ese sentido, pueden ser importantes al inicio de las actuaciones, en cuanto que permiten guiar la investigación hacia nuevas pruebas o a la identificación de sospechosos o la víctima. También pueden ser un medio importante para corroborar o invalidar otros tipos de pruebas relacionadas con los hechos del caso.

g) En cuanto al control previo al acceso a los datos, el 80% de los Estados miembros que participaron en el estudio cuentan con alguna forma de autorización previa obligatoria para que las fuerzas de seguridad accedan a los datos. Normalmente a través de una orden judicial o del ministerio fiscal. No obstante, hay excepciones a este requisito general, basadas en:
   i. el tipo de datos sin contenido. En cuatro países no son necesarias las solicitudes ex ante para los datos de los abonados;
   ii. el tipo de infracción investigada. En un Estado miembro, en el caso de los delitos menores, los servicios policiales (no así las autoridades judiciales) siempre requieren autorización judicial. En el caso de las infracciones penales, se requiere la autorización de la Fiscalía en los procedimientos previos al juicio y la autorización judicial durante el proceso judicial;
   iii. el tipo de agencia encargada de la aplicación de la ley que realiza la solicitud. En un caso, las autoridades de la policía, en el marco de una investigación penal, pueden acceder a todo tipo de datos sin autorización previa, mientras que en el ámbito puramente de seguridad, pueden acceder a los datos de los abonados sin autorización previa, pero necesitan autorización del fiscal para acceder a los datos de tráfico y de localización.

h) Los proveedores de servicios procesan las solicitudes siguiendo diferentes pasos, que incluyen la verificación de la solicitud, la extracción de los datos y su

transferencia a los servicios requirentes utilizando protocolos seguros, plataformas informáticas o formularios preestablecidos. En general, las solicitudes son gestionadas internamente por un departamento especializado (en la mayoría de los casos) que ha tenido que desarrollar sistemas informáticos específicos para almacenar, extraer y transmitir los datos. La mayoría de los operadores consultados realizan controles sobre las solicitudes que reciben, con diferentes grados de detalle.

Para cumplir con lo expresado en el párrafo anterior, los operadores de telecomunicaciones concernidos han tenido que invertir en el desarrollo de plataformas informáticas y en la automatización de procesos para responder a las solicitudes de forma eficiente. Sin embargo, el estudio refleja que el uso de puntos de contacto únicos (SPOC) por parte de las autoridades policiales no está muy extendido. De hecho, los proveedores pusieron de manifiesto la necesidad de una mayor normalización de los procedimientos y el uso de los SPOC, lo que aumentaría la eficacia de todo el proceso y sería rentable a medio y largo plazo.

i) Otra cuestión importante es la relativa a los procedimientos de acceso en investigaciones transfronterizas, que en la actualidad son muy frecuentes. Existen varios canales para el intercambio transfronterizo de este tipo de datos en la UE, siendo la Orden Europea de Investigación (OEI) y Europol los más utilizados. Los procedimientos transfronterizos plantean problemas a las autoridades competentes, los proveedores de servicios de Internet y los operadores de telecomunicaciones. Los servicios policiales critican la falta de normas armonizadas, la excesiva duración de los procedimientos para la obtención de los datos y la falta de conocimiento de las normativas; y las OTT *(Over-the-top, por sus siglas en inglés)*[624], que ofrecen servicios transfronterizos, también experimentan desafíos relacionados con los diferentes requisitos de seguridad en los distintos Estados miembros de la Unión Europea

[624] OTT significa *"Over The Top"* y se trata de un servicio de libre transmisión. Es decir, plataformas que emiten contenido a través de internet sin necesidad de recurrir a operadores tradicionales de difusión. Para conectarse a estos servicios OTT solo se necesita un dispositivo (o aplicación compatible) y conexión a Internet.

en el caso del almacenamiento centralizado de información (por ejemplo, requisitos de localización de datos) y respecto de los diferentes regímenes de retención.

De hecho, respecto de este nuevo tipo de operadores particulares, que son cada vez más utilizados por los ciudadanos y también por los delincuentes, se extrajeron también algunas conclusiones interesantes en el estudio:

i. Los procedimientos descritos anteriormente para los proveedores clásicos de servicios de telecomunicaciones pueden aplicarse en cierta medida a las OTT, incluso en ausencia de marcos jurídicos nacionales o de la Unión que impongan a estos últimos una obligación general de conservación de datos con fines policiales. En respuesta a una solicitud de acceso, las OTT pueden proporcionar a las fuerzas de seguridad una serie de datos no relacionados con el contenido, que conservan para sus propios fines empresariales o comerciales.

ii. Aunque las OTT no tienen ninguna obligación de informar sobre el número de solicitudes de acceso, a menudo lo hacen en sus informes de transparencia. En general, publican estadísticas semestrales. La mayoría de las solicitudes provienen de dos de los Estados miembros participantes[625]. Respecto de otros países, llama la atención que envían muchas solicitudes en comparación con la relativamente pequeña cifra de habitantes. En cualquier caso, las OTT reciben muchas menos solicitudes de acceso que operadores clásicos en el 90% de los países entrevistados, lo que nos llama la atención teniendo en cuenta, como decimos, que actualmente son los servicios más utilizados por los ciudadanos para comunicarse y, por tanto, también por los delincuentes para cometer sus delitos o comunicarse también entre ellos, máxime cuando la mayoría de estos servicios que ofrecen las OTT son cifrados de extremo a extremo.

[625] Tanto en cifras absolutas como en relación con su población total.

iii. Las OTT tienen tasas de rechazo de solicitudes similares a las de los operadores clásicos y sus motivos de rechazo son también parecidos. En la mayoría de los casos, la denegación se basa en que no localizan los datos que se les solicitan[626].

iv. En cuanto a sus procedimientos, al igual que los clásicos, han establecido también procesos internos y centralizados para recibir, seguir, procesar y responder a las solicitudes de las agencias encargadas de la aplicación de la ley. Se utiliza un sistema interno de verificación para comprobar si las solicitudes de acceso a los datos son válidas, es decir, si proceden de una fuente legítima y tienen una base jurídica legítima. Según el estudio, este sistema de verificación es la parte más compleja y laboriosa del procedimiento de acceso a los datos [si bien, no hemos llegado a conocer el motivo para tal afirmación]. Las OTT también piden el uso extensivo entre los Estados miembros de los SPOC como una forma de agilizar los procedimientos y racionalizar los costes del mantenimiento y gestión del sistema de colaboración establecido.

j) También se tuvo en cuenta en el estudio una mirada hacia el futuro para pulsar la opinión de los involucrados de cara a los avances tecnológicos futuros y la medida en que afectarían al objeto de nuestro estudio:

i. En relación con los desarrollos que más afectarán a corto y medio plazo a la conservación de datos con fines de persecución del delito, señalaron *"el cifrado de extremo a extremo (E2EE) y el uso de direcciones IP dinámicas, seguidos por el despliegue del 5G y otras aplicaciones tecnológicas relacionadas, como el Big Data, el Internet de las cosas (IoT) y el blockchain"*. Este creciente cambio de las comunicaciones de los servicios de telecomunicaciones tradicionales a los servicios OTT, que a menudo están sujetos a E2EE, plantea desafíos particulares para la investigación y el enjuiciamiento penal de delitos graves y aumenta la importancia del acceso a

[626] Bien porque no conservaron los datos solicitados o porque, habiendo hecho, ha transcurrido el tiempo de almacenamiento y han sido borrados.

los metadatos. A ello se suma la falta de expertos en tecnologías de la información cualificados para este tipo de avances.

ii. Una consecuencia inmediata de la introducción de la 5G que identificaron todos los participantes (y vinculada a las OTT y a las agencias de aplicación de la ley) es el gran aumento de la información potencialmente relevante para los servicios policiales en el marco de sus investigaciones, con las consiguientes implicaciones en las infraestructuras y los costes de almacenamiento, seguridad y gestión. La 5G utilizará probablemente interfaces y protocolos encriptados, lo que significa que los datos sobre los que estamos trabajando, normalmente disponibles con la tecnología actual (especialmente los datos de identificación), podrían dejar de estarlo. Además, la arquitectura de la red 5G (fragmentada y virtual), impedirá que los proveedores de servicios tengan una copia completa de la información disponible, a menos que se les imponga la obligación. Esto presentaría nuevos motivos de preocupación, adicionales, que afectarían negativamente a la cooperación, en general, y a los procedimientos transfronterizos, en particular.

iii. Por otro lado, los retos relacionados con los servicios de la Internet de las Cosas (IoT) a menudo se derivan de las mayores cantidades de datos disponibles y de la naturaleza transfronteriza de tales servicios[627]. Se observó que, mientras que los operadores de telecomunicaciones se esfuerzan por asignar normas de retención de datos a sus servicios de IoT en diferentes jurisdicciones, los investigadores policiales experimentan dificultades para obtener información a través de mecanismos transfronterizos, puesto que solicitan datos transfronterizos (normalmente a través de las OEI) y se enfrentan a tiempos de espera más largos para acceder a ellos, a la incertidumbre sobre la disponibilidad de esos datos en otro país (los

[627] Por ejemplo, el gran volumen de datos generados por las tarjetas SIM de los coches, que se recopilarán en varios países, ya que es probable que los coches circulen entre los Estados miembros, mientras que los servicios relacionados con las tarjetas SIM probablemente se presten a través de una plataforma centralizada.

diferentes marcos nacionales pueden tener periodos de conservación más cortos o pueden no conservar determinados tipos de datos), además de la preocupación sobre la legitimidad de dichas solicitudes en otro país.

En conclusión, aunque, como indicábamos al principio del apartado, no disponemos de los datos ni del parecer de todos los Estados miembros de la Unión, creemos que la información disponible presenta una imagen nítida y, al mismo tiempo, preocupante, sobre las consecuencias de no poder armonizar las reglas sobre conservación de metadatos, así como el acceso a los mismos con fines de investigación penal y enjuiciamiento de delitos; además de que, aunque se homogenicen las normas, no existe información sobre la que realizar una solicitud con autorización judicial, porque los proveedores de servicios no podrán conservar datos valiosos (incluso fundamentales para algunos delitos cometidos a través de servicios de Internet):

- A falta de seguridad jurídica en los marcos legales nacionales sobre conservación de datos, existe el riesgo de que las fuerzas de seguridad no puedan acceder a pruebas importantes necesarias para investigar y perseguir delitos. Las diferencias existentes en las legislaciones nacionales parecen plantear problemas para los casos de investigaciones transfronterizas, en los que las fuerzas de seguridad se enfrentan a diferentes procedimientos y períodos de conservación entre países.

- Períodos de conservación poco claros e insuficientes en el caso del almacenamiento de datos con fines comerciales. Esto es especialmente problemático en los países que no tienen la obligación legal de que los operadores conserven los metadatos, ya que los servicios policiales no pueden saber con certeza qué datos estarán disponibles y durante cuánto tiempo[628]. Estos periodos de conservación podrían no ser suficientes para la investigación de delitos cometidos fundamentalmente en línea o de delincuencia organizada transfronteriza, que a menudo se detectan mucho más tarde. En consecuencia, algunos delitos cometidos por medios electrónicos (sobre todo en los Estados

[628] De media, se conservan durante tres meses.

miembros que no tienen obligación de conservar los datos) no se persiguen y algunos delitos pueden ni siquiera detectarse.

- La clasificación de los diferentes tipos de datos (datos de abonado, tráfico y localización) es similar en todos los Estados miembros, lo que facilita a las autoridades locales y a los proveedores de servicios de telecomunicaciones la gestión de las solicitudes de acceso a los datos. Sin embargo, la clasificación de datos como los números de identificación de la tarjeta SIM y del dispositivo (por ejemplo, IMSI, IMEI), la dirección IP y el número de puerto para las direcciones IP dinámicas es más incierta; especialmente las dinámicas, que son las más difíciles de obtener.

- La definición o clasificación de los datos en determinados Estados miembros tiene influencia sobre los requisitos de acceso[629].

- Como indicábamos antes, en la práctica, los datos se suelen solicitar tras una evaluación por los investigadores, solo cuando son necesarios o en función de la gravedad del delito, incluso en aquellos Estados miembros que menos restricciones tienen en base a su legislación nacional.
- Las tareas de supervisión de la retención, suele ejercerse de forma compartida por las agencias de protección de datos y los reguladores del sector de las telecomunicaciones. Sin embargo, el alcance de sus respectivas competencias sobre las OTT no siempre está claro.

- En los casos en que los proveedores de servicios y las agencias encargadas de la aplicación de la ley han desarrollado procedimientos y procesos automatizados, como plataformas informáticas y SPOC, estos sirven para facilitar el acceso seguro a los datos. Sin embargo, no está extendido y el sector ha solicitado una mayor normalización de los procedimientos y el uso de los SPOC. En investigaciones transfronterizas, se añade dificultad, debido a las diferencias en

[629] Por ejemplo, las solicitudes de acceso a los datos de los abonados no requieren una autorización previa.

los sistemas nacionales de conservación y el desconocimiento de las prácticas procesales entre los diferentes servicios policiales y de investigación.

- En determinadas ocasiones (frecuentes) el único recurso disponible es acudir a la conservación rápida o *quick freeze*. Sin embargo, no puede sustituirla totalmente, ya que solo puede aplicarse a partir del momento en que se detecta o se sospecha un delito y depende de que los datos sean realmente almacenados por los proveedores de servicios electrónicos.

- Algunos proveedores de servicios de comunicación están excluidos de las obligaciones generales de conservación de datos y las OTT también. Esta situación podría cambiar con la aprobación del reglamento de privacidad de las comunicaciones que sigue en fase de discusión entre los colegisladores. Sin embargo, no está claro hasta qué punto los Estados miembros tendrán que incorporar este requisito a su legislación.

- Los retos tecnológicos existentes, como la conservación de direcciones IP dinámicas, siguen sin resolverse, mientras que los próximos avances tecnológicos (como la 5G y la IoT) probablemente complicarán algunos de los problemas existentes para la conservación de datos los datos objeto del estudio. La 5G también traerá consigo nuevos retos, ya que su arquitectura basada en el servicio dificultará a los proveedores el suministro de ciertos tipos de datos que actualmente se conservan, como los números IMSI.

- Se espera que la prestación transfronteriza de servicios de comunicación aumente aún más con la implantación de las aplicaciones de IoT habilitadas por la red 5G. En consecuencia, exigirá también incrementar el recurso a las investigaciones transfronterizas y acudir a los mecanismos de cooperación policiales existentes, para los que el estudio considera que los procedimientos actuales no son adecuados. Los próximos retos tecnológicos podrían suscitar nuevas preocupaciones y plantear la necesidad de un enfoque europeo también de esta cuestión.

CAPÍTULO IX. PROPUESTAS PARA UN NUEVO SISTEMA EUROPEO DE CONSERVACIÓN DE METADATOS CON FINES DE LUCHA CONTRA LA DELINCUENCIA GRAVE

1. Consideraciones generales

Ocho años después de que el TJUE declarase la invalidez de la Directiva sobre la conservación de datos, es necesaria una solución. Sin embargo, no parece que haya una idea clara de cómo proceder a nivel europeo, ni tampoco en los Estados miembros, a tenor de las sucesivas cuestiones prejudiciales planteadas ante el Alto tribunal y que, a medida que se van sustanciando, al margen de algunas precisiones, no hace más que confirmar y afianzar la doctrina fijada ya en 2014 y 2016. Al menos a medio plazo (aunque en el último año, quizás a la espera de nuevos pronunciamientos de Tribunal, se ha retirado de las agendas de discusión entre los expertos) continuarán los debates en el seno de las instituciones europeas, fundamentalmente en el Consejo (en conexión directa con la Comisión), sobre las distintas opciones y claves que permitan dibujar una posible solución de compromiso entre los Estados miembros y que respete los criterios establecidos y reiterados por el Tribunal de Luxemburgo.

Al margen de cómo evolucione la situación, teniendo en cuenta los límites y los puntos clave sobre los que tendrá que pivotar la solución o soluciones hacia un nuevo régimen de conservación de datos de tráfico y de localización (incluidos aquellos otros que permiten identificar la IP de origen de una comunicación y la identidad civil de quienes participan en una comunicación), las opciones sobre las que habrá que debatir y decidir no son demasiadas y cada una de ellas [como todo en la vida] tiene ventajas e inconvenientes. Pero consideramos y defendemos que no es discutible ya en estos momentos que el *nuevo* sistema de conservación y acceso a estos metadatos no volverá a ser el mismo que antes, ni con las posibilidades que para ciudadanos y agencias encargadas de la aplicación de la ley ofrece la tecnología actual ni ante los nuevos desarrollos que ya están en fase de prueba o en funcionamiento y que, probablemente, dificultarán más aún la situación (cifrado de extremo a extremo, CGNAT, IoT, 5G, IA, etcétera).

En las distintas sentencias analizadas, si bien se ha reconocido que algunas medidas de conservación de datos son permisibles en virtud del Derecho de la Unión, se ha confirmado que la conservación y transmisión generales e indiferenciadas de datos de tráfico y de localización están, en principio, prohibidas por el derecho europeo. Sin embargo, también se han especificado, como venimos reiterando, aquellas formas concretas de conservación (sujetas a estrictas salvaguardias) que podrían ser compatibles con ese derecho, especialmente en función de dos cuestiones básicas:

- La finalidad de la conservación: la seguridad nacional, incluido el terrorismo; y la delincuencia grave y las amenazas a la seguridad pública en general; y
- Las categorías de datos que deben conservarse: datos de tráfico y de localización, direcciones IP del origen de la conexión y datos de identidad civil.

Además de lo anterior, el Tribunal ha fijado una serie de criterios o principios generales que deberán ser tenidos en cuenta en cualquiera de las opciones que se consideren para que estas sean respetuosas también con los derechos fundamentales afectados:

- control previo de acceso a los datos conservados, salvo supuestos muy específicos en los que pueda concederse a posteriori;
- información a las personas afectadas por la injerencia en sus derechos, con la excepción de que pueda afectar negativamente a las investigaciones y;
- establecimiento de garantías de seguridad sobre los datos conservados para evitar accesos indebidos o ilícitos.

Sobre esta base, consideramos (en sintonía con las propuestas defendidas también por los expertos en las discusiones en el seno de las instituciones europeas) que se debe tomar una decisión por parte de los Estados miembros en el marco del Consejo de la Unión Europea –a nivel técnico- respaldada por el apoyo político de los ministros del interior –en el Consejo JAI- y, al más alto nivel, por los jefes de estado y de gobierno –en el Consejo Europeo- sobre una de las opciones generales que reflejamos a continuación, de forma que, una vez elegida la más idónea (de acuerdo con los mecanismos propios de toma de decisiones en el ámbito comunitario; no siempre fáciles), se pueda diseñar de forma precisa y revestir de todas las garantías necesarias

que permitan su duración en el tiempo, su defensa ante cualquier juicio de legalidad al que pudiera ser sometido por el Tribunal de Justicia de la Unión Europea o por alguno de los tribunales nacionales, y que pudiera evolucionar de forma flexible ante los avances tecnológicos a los que las sociedades actuales estamos acostumbrados y, por qué no, también ante el avance en la protección y garantía de los derechos y libertades fundamentales de los ciudadanos europeos:

1.1 ¿Abordar la situación desde una perspectiva puramente nacional?

Puesto que no ha sido posible hasta ahora encontrar una solución europea que permita continuar con el régimen anterior de conservación de datos, bien porque el Tribunal europeo no ha modificado su doctrina inicial tras la *Sentencia Digital Rights*, o porque los Estados miembros no han llegado a un consenso sobre cómo proceder en el futuro con otras alternativas de investigación diferentes a las que se apoyan en los metadatos de las telecomunicaciones; y unido al hecho de que las iniciativas que hasta ahora se han puesto en marcha lo han sido a nivel individual (a través de la aprobación de una norma diferente -o modificada- a la que nació de la transposición de la Directiva invalidada o continuando con el paraguas de las normativas nacionales vigentes antes de la anulación de la Directiva de 2006), parece lógico que una de las opciones sobre la que reflexionar sea la que apuesta por no desarrollar ninguna iniciativa legislativa a nivel de la Unión Europea.

En este caso, la Comisión se abstendría de cualquier actuación proactiva y correspondería a los Estados miembros abordar las consecuencias de las sentencias a nivel nacional, de acuerdo con la Carta de los Derechos Fundamentales y la jurisprudencia del TJUE, para de esa forma tener en cuenta las especificidades nacionales. Aun así, la Comisión podría jugar un papel activo y apoyar a los Estados miembros en este proceso, por ejemplo, facilitando los intercambios de información entre países, organizando reuniones de expertos para poner en común las dificultades que se vayan observando (también las buenas prácticas y experiencias positivas) y las acciones que se puedan estar llevando a conocimiento del Tribunal europeo u otros tribunales nacionales y sobre las que se puedan extraer conclusiones válidas para todos; o incluso también reunir a otras partes interesadas: el sector de las telecomunicaciones,

expertos en protección de datos, en nuevas tecnologías y nuevos desarrollos para las comunicaciones electrónicas, etcétera, para conocer sus puntos de vista y argumentos y que estos puedan ser tenidos en cuenta por los Estados miembros ante la eventual modificación de sus normativas nacionales. En esta labor, consideramos que sería relevante la participación de EUROPOL, a través de su Centro Europeo de Ciberdelincuencia, conocido entre los expertos policiales como EC3[630], por su rol de coordinador de las actividades policiales transfronterizas contra la ciberdelincuencia y su especialización en tecnología al servicio de las agencias encargadas de la aplicación de la ley[631]; y también con la Red Judicial europea de cibercriminalidad (EJCN, por sus siglas en inglés), que juega un papel similar, en este caso dentro de EUROJUST, y desde el ámbito de jueces y fiscales[632].

1.2 ¿Coordinar a nivel europeo una acción nacional no vinculante?

Como en muchos otros ámbitos de discusión en el Consejo de la Unión Europea, especialmente ante materias muy complejas desde el punto de vista técnico o con gran carga política (ante las que existen posiciones muy marcadas y contrarias entre algunos Estados miembros o entre grupos de países que se organizan por bloques geográficos tradicionales) es difícil encontrar una posición común y consensuada que permita conciliar todos los intereses en juego y los expedientes se alargan en el tiempo (hasta el punto de que, en ocasiones, se debe decidir entre la opción de abandonar la propuesta, después de meses o incluso años de debate; o rebajar las expectativas iniciales y adoptar acuerdos muy generales, que en ocasiones desdibujan completamente la iniciativa original de la Comisión; o ejercer presión entre grupos de países sobre otros expedientes que tengan relación, para forzar un acuerdo que finalmente no satisface a nadie, pero que permite llegar a un consenso.

[630] En Europol existe el conocido como EC3 *(European Cybercrime Centre)*, que fue concebido para reforzar y mejorar la respuesta de las agencias encargadas de la aplicación de la ley en la Unión Europea en la lucha contra el cibercrimen y la protección de los ciudadanos europeos, sus negocios y los gobiernos de los Estados miembros. Para profundizar, vid. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[631] Para profundizar sobre el EC3, vid. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, consultada el 14 de octubre de 2022.

[632] Para profundizar sobre la EJCN, vid. https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network, consultada el 14 de octubre de 2022.

En este expediente concreto, aunque casi todos (quizás todos) los Estados miembros están alineados en las grandes cuestiones sobre las que se debe actuar y también sobre los problemas que la *nueva* situación está creando en la labor de prevención y lucha contra la delincuencia grave en la Unión Europea, no se ha conseguido obtener una idea clara sobre cómo proceder; tampoco existe una propuesta concreta al respecto presentada por la Comisión, que percibe que hay que hacer algo, pero no sabe qué. En cambio, sí hay orientaciones políticas y un impulso decidido alentando a que se aborde con prontitud y se encuentre una solución respetuosa con la Carta y con los criterios marcados por el Tribunal europeo. Eso sí, también eficaz a los efectos antes citados.

En estas situaciones, en ocasiones la Comisión suele recurrir a la presentación para aprobación por el Consejo de unas *"Orientaciones"* a nivel europeo. En definitiva, la institución europea con competencia para presentar propuestas normativas redacta un documento con el que pretende *guiar* la acción de los Estados miembros. En el caso objeto de nuestro estudio, creemos que, si se optara por esta solución, las orientaciones deberían abarcar los distintos supuestos relativos a todos los fines y categorías de datos, de forma que incluyera y resumiera [aunque es conocido por todos los Estados miembros] el marco dibujado por la doctrina del Tribunal, contribuyendo así a dar respuesta a las distintas cuestiones que los tribunales nacionales han ido presentando ante el Tribunal de Luxemburgo (muchas de las cuales se han repetido de forma sucesiva, aunque presentadas por diferentes Estados miembros amparándose en la casuística propia de sus leyes nacionales, y que ha obtenido una contestación casi idéntica por parte del Tribunal). El objetivo, por tanto, sería *guiar/orientar* a los Estados miembros en la adaptación de sus normas a las resoluciones del Tribunal y trasladar un mensaje de que ya no hay vuelta al pasado y, al menos a corto plazo, tampoco hay una solución general que satisfaga plenamente a todos.

Una de las ventajas de este enfoque es que podría llevarse a cabo en menos tiempo del que se tarda en elaborar una evaluación de impacto y redactar, negociar, aprobar y poner en funcionamiento una nueva legislación. Proporcionaría además un margen de flexibilidad mayor para que los Estados miembros apliquen las orientaciones

en la adaptación de su normativa nacional a la doctrina ya consolidada, sin cercenar la posibilidad de una propuesta legislativa europea en un futuro más o menos próximo. Como contrapartida, aunque este tipo de documentos suele incluir en gran medida el parecer común de los Estados miembros (puesto que antes de aprobarse por la Comisión, se reúne a los expertos en aras a *garantizar* una mayor eficacia en la adopción de las medidas, con carácter voluntario, que en el texto se incluyen), no dejan de ser recomendaciones y, en consecuencia, no son jurídicamente vinculantes ni directamente ejecutables.

Al menos en una primera fase, las soluciones reales se dejarían a los Estados miembros. Este hecho aporta flexibilidad, pero también disparidad en la ejecución, por lo que se perdería uno de los objetivos fundamentales que la Unión persigue en la adopción de políticas comunitarias en materia penal y de cooperación policial, como es la armonización de la actuación ante fenómenos o situaciones de alcance europeo y/o global; pero al mismo tiempo permitiría probar soluciones a nivel nacional, con la eventual participación del TJUE y la posibilidad de que su doctrina evolucione de forma más favorable para la lucha contra la delincuencia grave y otras amenazas a la seguridad pública. La desventaja principal, sin embargo, es que cada solución se verá como un intento nacional, no como algo que se apoya explícitamente desde la Unión Europea, además de que, sin duda, ante el convencimiento que mostramos respecto de que las soluciones a la amenaza de la delincuencia grave transnacional no se pueden tratar a nivel nacional, se resentiría gravemente la eficacia de las actuaciones policiales y judiciales y, repercutiría negativamente en la protección de la seguridad de los europeos y en la defensa de algunos de sus derechos y libertades fundamentales. Por último, la falta de armonización y las divergencias de las soluciones nacionales acabarían afectando también al mercado interior, que precisamente pretendía armonizar la Directiva 2006/24/CE, y dificultaría el intercambio de información y la colaboración entre agencias europeas encargadas de la aplicación de la ley.

1.3 ¿Adoptar una nueva norma europea de conservación de metadatos?

La tercera opción lógica -que después de la investigación que hemos realizado y que llega ahora a su fin, defendemos- es la adopción de una norma a nivel de la Unión

que establezca un sistema europeo de conservación de metadatos de las comunicaciones electrónicas que tenga en cuenta los requerimientos que el Tribunal ha fijado como imprescindibles para respetar los derechos y libertades fundamentales de los ciudadanos europeos y que sirva de base para la adopción de leyes nacionales eficaces en la lucha contra la delincuencia grave y ante las amenazas a la seguridad nacional. Esta opción, que entraremos a valorar con detalle, podría recoger todos los fines legítimos sobre los que el Tribunal se ha pronunciado o limitarse a alguno de ellos, teniendo en cuenta las especificidades de la seguridad nacional y la defensa.

La ventaja es clara en términos de armonización y también significaría un contundente compromiso político sobre lo que se entiende como el equilibrio adecuado. Sin embargo, requeriría no sólo una propuesta de nuevo instrumento, sino también un acuerdo entre los dos colegisladores en un sector en el que la experiencia pasada ha demostrado que las negociaciones son especialmente difíciles. Como se ha indicado, la jurisprudencia del Tribunal es en gran medida sólida ante este complejo asunto y ha evolucionado solo a través de pequeños matices. Existe un margen de discusión sobre la base de las *tonalidades* que ha venido introduciendo en las últimas sentencias, pero este margen de maniobra para discutir soluciones innovadoras es más bien limitado en el contexto de las relaciones interinstitucionales propias del procedimiento legislativo ordinario que se seguiría en la adopción del nuevo instrumento normativo.

2. Propuestas para un nuevo sistema europeo de conservación de datos de las comunicaciones electrónicas

Al analizar de forma conjunta las sentencias *Privacy Internacional y La Quadrature du Net* (y las posteriores que basan sus decisiones en gran medida en esta última), observamos que el Tribunal incluye la conservación con fines de protección de la seguridad nacional en el ámbito de aplicación de la legislación de la Unión, resolviendo de esa forma una cuestión que ha sido muy controvertida, tanto desde el punto de vista político y jurídico a nivel de los Estados miembros como desde el criterio de los expertos. Por otro lado, la sentencia en el caso *La Quadrature du Net* y las siguientes (de 2021 y 2022) establecen los límites a los derechos y libertades fundamentales recogidos en la Carta que se ven afectados por las medidas adoptadas en

esta materia, entre otras, las que se aplican al uso a nivel nacional de la excepción de seguridad nacional. Con ello, se crea un marco jurídico *revisado* en el que deben actuar las agencias encargadas de la aplicación de la ley. En cierto modo, se pone fin [o está próximo] a las resistencias de los Estados miembros a *acatar* las sentencias del Tribunal europeo, que continuaban presentando cuestiones prejudiciales sobre asuntos recurrentes y, en gran medida, ya resueltos. Como indican Mitsilegas, Guild y otros (2022; 2)[633], esta situación pone de manifiesto también la lucha política entre las instituciones de la UE y los Estados miembros sobre el futuro de lo que estos autores denominan la *"vigilancia masiva"*.

El Tribunal estableció distintos objetivos de interés público y los emparejó con diferentes medidas de retención de datos en base a su lectura de los diferentes niveles de amenaza y gravedad que denotan cada objetivo. En esa labor, distinguió entre la salvaguarda de la seguridad nacional y la seguridad pública como fines de la conservación de datos, considerando que la primera puede justificar medidas más intrusivas que las que pueden justificarse por otros objetivos. Además, al examinar los diversos objetivos para los que se retienen los datos de tráfico y de localización, se pueden distinguir tres grupos de objetivos de interés público – la seguridad nacional, incluida la prevención del terrorismo; la lucha contra la delincuencia grave, o la persecución y el enjuiciamiento de delitos menos graves- y cada uno de ellos corresponde a un grado diferente de amenazas en función de su naturaleza y gravedad, lo que puede justificar diferentes conjuntos de actividades de conservación.

Así, hemos visto que solo para la prevención de amenazas a la seguridad nacional ha considerado que, con las debidas salvaguardas, procedería una conservación generalizada e indiferenciada de datos. También ha diferenciado claramente los supuestos que se recogen bajo la protección de la seguridad nacional (o la defensa, de la que no hemos hablado) y otros supuestos, y que una conservación con un objetivo de protección de las estructuras básicas de un Estado no puede dar lugar al acceso a los datos con ocasión de otros fines, como podría ser la prevención o lucha contra la

[633] MITSILEGAS, V., GUILD, E, KUSKONMAZ, E. Y VAVOULA, N., *"Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks".* Eur Law J. 2022; 1-36. Doi:10.1111/eulj.12417, p. 2

delincuencia. Por tanto, no es este el supuesto que a los efectos de esta tesis nos interesa principalmente, sino el de proponer las bases para el nuevo marco de conservación de datos en la lucha contra la delincuencia grave. En consecuencia, creemos que la futura norma que regule la conservación de este tipo de datos debería dejar al margen la seguridad nacional, por sus especiales características [que hemos venido relatando] y porque, aunque el Tribunal ha determinado que no es ajena a la Directiva 2002/58/CE, creemos que la nueva propuesta normativa debería fundamentarse en el ámbito de la cooperación policial y judicial principalmente (o en combinación con las disposiciones de los Tratados respecto de la armonización del mercado interior) y, de esa forma, no mezclar supuestos que están relacionados pero que presentan características muy diferentes y que creemos que su regulación conjunta aportaría confusión, en detrimento de las medidas para la lucha contra la delincuencia. La seguridad nacional ofrece un margen de maniobra muy superior a los Estados miembros y en una norma diferenciada se podría regular de forma más apropiada la conservación general e indiferenciada *matizada* que permite el TJUE para esa finalidad.

Nos recuerda Ortiz-Pradillo (2020; 8 y 9)[634] que ya las Conclusiones de los Abogados Generales Sánchez y Pitruzzella (que luego se confirmó en las sentencias correspondientes) afirmaban que la seguridad nacional solo queda excluida de la aplicación de la Directiva de privacidad electrónica de forma excepcional, y pone como ejemplo: *"cuando se trate de técnicas de recopilación de información que sean aplicadas directamente por el Estado, pero no cuando se trate de normas que regulen las actividades de los proveedores de servicios de comunicaciones electrónicas imponiéndoles obligaciones específicas a tales empresas privadas"*. Es decir, la exclusión se extiende únicamente al ejercicio de esas competencias cuando se ejercen de *"manera directa y por sus propios medios"*. Entendemos que, en consecuencia, no cuando se impone una obligación a una tercera parte; en este caso, además, privada. Aunque esta misma situación podemos observarla respecto de las obligaciones que la Directiva PNR impone a las aerolíneas que operan en Europa, que recogen datos para sus fines comerciales y de negocio (entre otros) y que se ponen a disposición de forma obligatoria de las autoridades designadas para su tratamiento, de las agencias encargadas de la aplicación de la ley.

[634] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones...", op. cit. 1-28.*

La doctrina parece no cuestionar que el terrorismo constituye una de esas amenazas a la seguridad nacional [si preguntamos a un determinado número de personas, a buen seguro la mayoría de ellas responderían como primera opción indicando este fenómeno como una amenaza real y previsible a las estructuras de un estado y la normal convivencia de los ciudadanos][635]. En consecuencia, la legislación que prevea una conservación de acuerdo con este objetivo de prevención de la seguridad nacional, ofrecerá fundamentalmente mayor amplitud en cuanto su alcance respecto de las personas afectadas, más que por los datos que deberán ser conservados; en definitiva, será una conservación limitada en el tiempo (con carácter renovable), que deberá seguir un procedimiento de supervisión por una autoridad judicial o administrativa que reúna las características de independencia respecto de las agencias encargadas de la aplicación de la ley o de los servicios de inteligencia [en materia de seguridad nacional tienen un papel más relevante que en el resto de objetivos contemplados]; en cambio, los datos tendrán que estar correlacionados con cada caso concreto objeto de investigación o respecto del que se quieran establecer medidas de prevención. En consecuencia, los Estados miembros tendrán un papel determinante a la hora de valorar cada caso, siempre bajo criterios de necesidad y proporcionalidad, pero que, sin duda, ofrecerán respuestas muy variadas dependiendo del Estado miembro de que se trate. Eso hace que regular estas situaciones a nivel europeo no sea fácil ni quizás oportuno. No obstante, estamos de acuerdo con Sánchez Guarido y Maddion Medina (2020; 4)[636] en que no se puede olvidar que el TJUE ha reiterado que *"la inviolable seguridad del Estado no puede erigirse como comodín o excepción general para no cumplir… con cualquier norma que garantice la no menos importante intimidad y confidencialidad de la información, o que imponga medidas que impliquen el registro indiscriminado de datos"*.

[635] Estas salvaguardas derivan fundamentalmente del Dictamen 1/15 del Tribunal de Justicia (Gran Sala), de 26 de julio de 2017, emitido con arreglo al artículo 218 TFUE, apartado 11, sobre el Proyecto de Acuerdo entre Canadá y la Unión Europea, en https://curia.europa.eu/juris/document/document/.jsf?text=&docid=193216&doclang=ES, que ya hemos analizado en capítulos precedentes.

[636] SÁNCHEZ GUARIDO, A. y MADDIO MEDINA, A., *"El TJUE reabre el debate entre privacidad o seguridad nacional"*, Diario La Ley, nº. 9743, 2020, pp. 1-5, p. 4, en https://www.perezllorca.com/wp-content/uploads/2020/11/diario-ley-tjue-reabre-debate-privacidad-seguridad-nacional.pdf

Por el contrario, nos interesa sobremanera otro de los objetivos recogidos como excepción en la Directiva de privacidad electrónica (sobre el que el Tribunal ha establecido diferentes criterios y que abre una variedad de posibilidades), ya que, al no poder desplegarse medidas de conservación generalizada e indiferenciada, las actuaciones de los servicios policiales y las autoridades judiciales se han visto más afectadas. Nos referimos a la lucha contra la delincuencia grave o la persecución y el enjuiciamiento de delitos menos graves. Aquí es donde haremos propuestas que, como nos proponíamos al comienzo de este estudio, nos permitan aportar algún elemento a la difícil ecuación que representa el equilibrio entre la colisión de dos derechos o grupos de derechos, que recogíamos con la rúbrica *"Seguridad versus Libertad"*.

Adentrándonos ya en la lucha contra la delincuencia grave y en la prevención de amenazas o ataques graves a la seguridad pública, debemos tener en cuenta las directrices que a lo largo de las sucesivas sentencias ha ido dando el Tribunal y que básicamente se pueden concentrar en dos generales y una *técnica* y, sobre estas habrá de construirse el nuevo modelo:

- Solo se podrán conservar los metadatos en base a supuestos que habiliten una conservación selectiva o una conservación rápida.
- Estas acciones deberán estar autorizadas y supervisadas por una autoridad judicial o administrativa independiente, tras la correspondiente prueba de necesidad y proporcionalidad (caso por caso), tanto para la adopción de las medidas como para su prórroga, siempre que, a pesar de la evolución de la situación, persistan las circunstancias que motivaron la autorización.
- Se deberán establecer los mecanismos adecuados para que la información conservada goce de medidas de seguridad que impidan un acceso ilegítimo, así como que, una vez que los datos ya no sean necesarios, se destruyan.

Observamos que las tres directrices están enfocadas a la conservación de los datos. No hemos mencionado nada todavía del acceso a los datos ni de su tratamiento posterior, más allá del que realizan los propios proveedores de servicios al tener que conservar esa información y enviarla a las agencias de aplicación de la ley cuando sea requerida. Ese aspecto fundamental (segundo gran bloque que se ha visto afectado para

la anulación de la Directiva 2006/24/CE y sobre el que se ha pronunciado también el Tribunal) lo veremos posteriormente.

2.1 Consideraciones particulares para una norma que prevea la conservación de metadatos de las comunicaciones electrónicas con fines de prevención y lucha contra la delincuencia grave

De forma particular y a modo de lista numerada, presentaremos las piezas (ideas clave argumentadas) que deberán encajarse y conformar, a nuestro entender, el *puzle* que es el nuevo sistema de conservación de datos. Quizás en este momento encontremos que el contorno de cada pieza no está pulido, o que haya que recortar parte de alguno de los lados de una o varias piezas, o que falte o sobre alguna de esas piezas, pero creemos que constituye un punto de partida adecuado y necesario para llegar a mostrar una imagen bien delimitada, armónica y que ofrezca una realidad que, como ocurre con cada uno de los cuadros que observamos en un museo, aunque no guste a todos, sí a la mayoría, y permita ser valorado como modelo (aunque perfectible) en otras partes del mundo. Los actores que deberán perfilar y unir las partes del *puzle* están plenamente identificados, pero hasta ahora no han encontrado la mayoría de las piezas ni parecen tener en la mente la imagen final que quieren proyectar. Después habrá que redactar la memoria de cómo encajan entre sí y qué transmite la imagen a los distintos actores que en el aparecen; pero eso corresponderá a los legisladores del Consejo y del Parlamento Europeo, con la ayuda y el asesoramiento de todos aquellos expertos en este tipo de construcciones manuales (organismos consultivos, sector afectado, ciudadanos, agencias encargadas de la aplicación de la ley, etcétera).

Primera. La base jurídica deberá abarcar no solo al artículo 114 del TFUE, sino también al artículo 82. Si bien son datos necesarios para los fines comerciales y de facturación de los operadores de las telecomunicaciones, serán conservados también a los efectos mencionados en el epígrafe anterior y, por tanto, en el ámbito de la cooperación policial y judicial en la Unión Europea. De esa forma, como indicábamos en su momento, la norma será diseñada desde el principio no solo como medida de armonización del mercado interior, sino también como una medida dentro del ámbito penal. Es cierto que el Tribunal no observó que la fundamentación en el artículo 114

tuviera que derivar en la anulación de la Directiva, pero sí aportó argumentos que conviene tener en cuenta y, mediante una integración de ambas fundamentaciones (mercado interior y cooperación policial y judicial), se armará el sistema de una forma mejor desde su creación. Tendrá que ir acompañada de la habitual evaluación de impacto y recoger las necesidades y puntos de vista de todas las partes interesadas: el sector de las telecomunicaciones, determinadas asociaciones de ciudadanos, los órganos consultivos de la UE, el Supervisor Europeo de Protección de Datos y, por supuesto, los representantes de las agencias encargadas de la aplicación de la ley, además del correspondiente parecer inicial del Parlamento Europeo.

Segunda. Las medidas que recoja la norma europea constituirán una excepción a la Directiva 2002/58/CE, al haber quedado invalidada la Directiva 2006/24/CE. No obstante, en el momento de la redacción de esta propuesta se encuentra en fase avanzada (después de varios años de negociación) el futuro reglamento europeo que actualizará la Directiva de 2002. Por tanto, será necesario fijarse en la redacción final del reglamento (hemos analizado determinados artículos del borrador de orientación general del Consejo, de febrero de 2021) y la posibilidad de que algunas de las excepciones que recoge el actual artículo 15, apartado 1, de la Directiva de privacidad electrónica, quede fuera o redactado de una forma diferente. Algunos expertos que participan en el grupo de trabajo del Consejo de la UE que está analizando la situación[637] (entre ellos el representante español), consideran que la clave para el diseño de un nuevo marco regulatorio de conservación de datos se encuentra precisamente en el nuevo reglamento de privacidad electrónica. Insisten y argumentan que este debería recoger una *"cláusula habilitante"* que, atendiendo a los criterios marcados por el TJUE y con pleno respeto a los derechos fundamentales recogidos en la Carta, se pueda fijar una excepción al reglamento que permita un régimen de conservación lo más amplio posible. La dificultad estriba en que en las negociaciones del reglamento de privacidad electrónica participan expertos del sector de las telecomunicaciones y la aportación de los técnicos que representan a los servicios policiales y autoridades judiciales es muy reducida y, ni siquiera en ese punto, se encuentra consenso entre ambas partes (quizás por el diferente enfoque de partida de la propuesta: el desarrollo

[637] Grupo de trabajo del Consejo de la Unión Europea, sobre cooperación judicial en asuntos penales (Conservación de Datos).

del mercado interior y no la cooperación policial y judicial en el ámbito penal). Aun así, la redacción actual del borrador permite esa posibilidad, a expensas de cómo avance la negociación interinstitucional con el Parlamento Europeo.

Tercera. Es fundamental poder definir de forma más precisa el concepto de delito grave, tomando como referencia quizás (al menos como punto de partida) el incluido en la Directiva PNR, puesto que el fin que persiguen ambas normas (PNR y futura norma de conservación de datos) es muy similar: *"garantizar la seguridad y proteger la vida de los ciudadanos y, al mismo tiempo, crear un marco jurídico para la protección de los datos"*, y también parten de la misma imposición de una obligación del sector público al privado de conservar determinados datos que, bajo ciertas condiciones y con las adecuadas garantías, se ponen a disposición de las autoridades competentes. La Directiva PNR define el delito grave como *"los delitos incluidos en el anexo II*[638] *que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo al derecho nacional de un Estado miembro"*. De esta forma, se opta por un listado cerrado de delitos (modificable) y un umbral mínimo de pena de internamiento en prisión; de acuerdo con el derecho nacional, como corresponde a las materias de derecho penal.

[638] En la Directiva PNR se ha optado por un listado cerrado de delitos (incluidos en el anexo II) que se incluyen en el concepto de *"graves"*. No obstante, se permite a la Comisión Europea, mediante el procedimiento de *"comitología"* poder modificar el listado de forma más ágil que la modificación de toda la Directiva. Estos delitos son los siguientes:

Lista de los delitos a que se refiere el artículo 3, punto 9, de la Directiva: *"1. pertenencia a una organización delictiva 2. trata de seres humanos 3. explotación sexual de niños y pornografía infantil 4. tráfico ilícito de estupefacientes y sustancias psicotrópicas 5. tráfico ilícito de armas, municiones y explosivos 6. corrupción 7. fraude, incluido el que afecte a los intereses financieros de la Unión 8. blanqueo del producto del delito y falsificación de moneda, con inclusión del euro 9. delitos informáticos/ciberdelincuencia 10. delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas 11. ayuda a la entrada y residencia ilegales 12. homicidio voluntario, agresión con lesiones graves 13. tráfico ilícito de órganos y tejidos humanos 14. secuestro, detención ilegal y toma de rehenes 15. robo organizado y a mano armada 16. tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte 17. falsificación y violación de derechos de propiedad intelectual o industrial de mercancías 18. falsificación de documentos administrativos y tráfico de documentos administrativos falsos 19. tráfico ilícito de sustancias hormonales y otros factores de crecimiento 20. tráfico ilícito de materiales radiactivos o sustancias nucleares 21. violación 22. delitos incluidos en la jurisdicción de la Corte Penal Internacional 23. secuestro de aeronaves y buques 24. sabotaje 25. tráfico de vehículos robados 26. espionaje industrial".*

La gravedad del delito es la clave para incluir bajo la rúbrica de *"prevención y lucha contra la delincuencia grave"* los supuestos que, sometidos a la correspondiente prueba de proporcionalidad, servirán a jueces y/o autoridades administrativas independientes habilitadas para determinar la eventual conservación de datos. Somos conscientes de la dificultad de alcanzar un consenso a nivel europeo a este respecto, por la propia reticencia de los Estados miembros a armonizarlo dada la diversidad de tradiciones legales nacionales, pero igual que se ha obtenido para otras normas, podría hacerse también en este caso. El borrador actual de reglamento de privacidad de las comunicaciones electrónicas, en el artículo que prevé las excepciones (artículo 11) se refiere a delincuencia, sin el adjetivo de *grave.*

Cuarta. La mayor o menor cantidad de tipos de datos que se conserven y sobre los que autorizar el acceso influirá sobre la capacidad de los investigadores para efectuar un análisis más completo de la actividad de los sujetos afectados y trazar un perfil más detallado y, en consecuencia, exigirá una mayor ponderación también sobre el alcance de la medida; es decir, no podrá ser aplicable a todos los casos, sino que la restricción deberá ser más o menos intensa según cada caso concreto, que habrá de ser analizada por el juez o la autoridad autorizada que entienda del caso planteado. Advierte con acierto Ortiz-Pradillo (2010;89)[639] que la más intensa intromisión en la intimidad provocada por las nuevas tecnologías, a diferencia de las intervenciones telefónicas clásicas, no puede quedar fuera de la exigencia de ponderación; sin duda, ese ha sido uno de los principales elementos de análisis del TJUE, como ha quedado de manifiesto en las sentencias dictadas.

Respecto de la determinación de las categorías de datos que son imprescindibles para contribuir a la lucha contra la delincuencia grave, ya hay una primera aproximación entre los expertos policiales, pero no hay consenso cerrado al respecto, al menos sobre aquellos que no aportan valor añadido y que se podrían excluir. Proponemos que EUROPOL ejerza el liderazgo en esta materia y, como ya hizo en 2017, reúna a los

[639] ORTIZ-PRADILLO, J.C., *"Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de datos de tráfico de las comunicaciones electrónicas"*, en La Ley Penal, nº. 75, octubre 2010, p. 80-94, p.89.

expertos policiales con experiencia en la labor de investigación hasta alcanzar un listado de los datos que son recogidos actualmente por los operadores de telecomunicaciones para sus fines de negocio y que servirán también para las investigaciones; otro con los datos que no sirven a intereses comerciales pero sí a efectos de investigación; y otro con datos prescindibles, bien porque su rendimiento es escaso o porque la información que aportan se puede obtener por otros medios de investigación. En esta propuesta nos remitimos al listado de las pinas 295 a 296 de este estudio, como punto de partida sobre el que seguir avanzando, bajo el asesoramiento y apoyo del EC3 de EUROPOL. Es necesario vencer la resistencia a no dejar de lado ningún dato, puesto que la situación (como decíamos antes) no volverá a ser como antes y la evolución tecnológica hará que determinados datos que ahora se consideran fundamentales, en un futuro próximo ya no sean necesarios o no estén disponibles [pongamos como ejemplo –aunque queda fuera de la Directiva de 2006 y del objeto de esta tesis- la suma importancia del contenido de las comunicaciones de voz a través de la red telefónica, cuyo acceso actualmente se ve muy comprometido por el progresivo abandono de las comunicaciones de voz a través de las llamadas de teléfono tradicionales –fijo y móvil- y su sustitución por el cada vez más extendido uso de mensajes dictados o de llamadas a través de aplicaciones y/o redes sociales, que operan con técnicas de cifrado de extremo a extremo][640]. Esto obliga a agudizar el ingenio y buscar otros medios de investigación que complementen las técnicas y el uso de los medios actuales al alcance de los servicios policiales y de inteligencia. Más adelante nos referiremos otros medios de investigación que, sin estar sometidos actualmente a la norma europea de privacidad electrónica, también pueden aportar una información fundamental en la prevención y lucha contra la delincuencia grave, a través de datos conservados por los operadores de esos servicios.

Sí es indudable y perentorio incluir esos nuevos servicios a los que nos referíamos antes (no recogido en la Directiva invalidada), como son las OTTs. Al margen de su uso cada vez más habitual, es relevante también la información que

[640] En el estudio que encargó la Comisión, que hemos citado en el capítulo anterior, se recoge una tabla con los tipos de datos (sin contenido) en función del mayor o menor uso por los investigadores, de forma que puede servir también de base a los expertos para valorar qué datos pueden ser prescindibles y cuáles imprescindibles. A modo de ejemplo, podemos resumir que los datos de suscripción e identificación de la comunicación son fundamentales, mientras que los datos localización, solo algunos de los que se conservan.

podrían aportar[641]. Al no estar sometidas a normativa alguna sobre conservación, los periodos en que cada una de ellas almacena los datos está establecida de forma individual, lo que obligaría a mantener reuniones para intentar armonizar sus intereses con los de los servicios policiales, con la dificultad añadida derivada de que muchos de estos proveedores de servicios tienen su sede fuera de la Unión Europea.

Quinta. El tiempo por el que se autoriza el acceso tiene un efecto directo sobre la injerencia en los derechos de los investigados. En ese sentido, es importante la Sentencia en el *Caso Ministerio Fiscal*, ya que tuvo en cuenta que la injerencia no fue grave por cuanto el acceso fue por un breve periodo de tiempo. Cita Ortiz-Pradillo (2020; 24 y 25)[642] una sentencia de la Corte Suprema de los EE. UU., que en 1983 ya tuvo en cuenta esta consideración (la escasez de tiempo) para determinar que no era necesaria autorización judicial para instalar un dispositivo de seguimiento por posicionamiento GPS, mientras que en 2012 se pronunció en sentido contrario, en otro caso similar en el que se habían controlado los movimientos de un sospechoso mediante un sistema similar de geolocalización durante casi un mes y las veinticuatro horas de día. Pues bien, en otra sentencia posterior (de 2018) respecto del acceso a datos conservados por los proveedores de servicio de telecomunicaciones, la Corte norteamericana consideró que la injerencia en los derechos a la privacidad es mucho mayor que la que se produce con los datos de posicionamiento GPS, al permitir conocer no solo los movimientos de una persona, sino [una vez más] porque permite establecer perfiles muy específicos y concretos de la vida y de sus vínculos familiares y personales, en aspectos tan protegidos como pudieran ser los relacionados con la religión, la política o las prácticas sexuales. En definitiva, este aspecto está más bien relacionado con la determinación, por el juez o autoridad administrativa habilitada, de la

[641] i) Datos del abonado: información de registro y del abonado, como: nombre de usuario/cuenta, dirección de correo electrónico, país, código postal, teléfono asociado, información de facturación y de transacciones de facturación (puede incluir la dirección de facturación y el método o instrumento de pago, registros IP, servicios utilizados, número de serie, historial de compras, información del dispositivo, etcétera; ii) Datos de tráfico: tipo de servicios utilizados, tipo de comunicación, registros de transacciones, registros históricos de detalles de llamadas recibidas y realizadas, registros de invitaciones de llamadas, etcétera, registros de invitaciones de llamadas, registros históricos de detalles del servicio de mensajes cortos (SMS), registro histórico de la actividad de intercambio de correo electrónico, actividad, registros de conexión e inicio de sesión con direcciones IP, posible historial de conexiones IP, etcétera; iii) Datos de localización: si son relevantes para los tipos de servicios.

[642] ORTIZ-PRADILLO, J.C., *"Europa: Auge y caída de las investigaciones penales…", op. cit.*, pp. 24 y 25.

gravedad de la injerencia en los derechos fundamentales y con la decisión de permitir o no el acceso a los datos almacenados.

Sin embargo, aquí nos referimos al periodo de conservación de los datos, que es un elemento tradicional de discusión en la negociación de los expedientes legislativos en la Unión Europea entre los colegisladores. Los expertos policiales siempre quieren aprobar periodos de conservación lo más largos posible (lo que parece aceptable desde la lógica de que el conocimiento de los delitos no siempre se produce en fechas próximas a su comisión, o por la frecuente extensión en el tiempo de las investigaciones complejas o de delincuencia organizada) mientras que el Parlamento Europeo no suele encontrar justificación para aceptar esas propuestas, por considerarlas desproporcionadas. En cualquier caso, para nuestro *puzle*, se deberá fijar un período de conservación lo más ajustado posible a ambos intereses, con la prevención fundamental de que se puedan emitir sucesivas órdenes para prorrogar la medida, debidamente autorizadas por la misma autoridad que solicitó la conservación y tras el análisis del cumplimiento de las mismas circunstancias que lo motivaron u otras de la misma entidad, en términos de necesidad y proporcionalidad. Proponemos que, una vez establecida la definición de delito grave (mediante una solución similar a la prevista en la Directiva PNR y con posibilidad de modificación de forma ágil por el procedimiento de *comitología*) y el listado de categorías de datos al que nos referíamos en el punto anterior, se pueda asignar un período de conservación inicial diferente en función de la importancia relativa de los datos que se haya previsto en ese listado, su sensibilidad y su contribución al esclarecimiento de las conductas delictivas graves.

No obstante, si bien defendemos que es obligatorio fijar un período de conservación de datos y diferenciar entre categorías, no podemos obviar que el tiempo de conservación no parece excesivamente relevante en sí mismo en cuanto a la injerencia en los derechos fundamentales afectados. El TJUE, en sus sentencias más recientes se ha pronunciado con el siguiente tenor: *"la conservación de los datos de tráfico o de localización […] es, en todo caso, grave, con independencia de la duración del período de conservación, de la cantidad y de la naturaleza de los datos conservados, cuando ese conjunto de datos pueda permitir extraer conclusiones muy*

precisas sobre la vida privada de la persona o personas afectadas" (apartado 89, STJUE SpaceNet). En consecuencia, incluso períodos muy cortos de conservación, como los que introdujo Alemania en su ley de 2011[que valoramos del todo insuficientes para cumplir la función para la que se produce su almacenamiento], han sido cuestionados por el Tribunal. Consideramos que lo realmente importante entonces es que los periodos iniciales, por cortos que sean, puedan ser prorrogados en cada caso concreto. Y, en base a la justificación del Tribunal europeo, nada obsta para que el punto de partida quede fijado en torno al periodo inicialmente introducido en los debates de la Directiva 2006/24/CE: quizás un año para los esenciales y que no forman parte de los que los proveedores utilizan para sus fines de negocio y comerciales, y seis meses o veinticuatro para los más sensibles de los esenciales y para los que ya recogen de oficio los proveedores, respectivamente. El periodo por el que se almacena este tipo de datos comerciales y de uso interno de las compañías del sector es probable que sea más amplio incluso, por lo que los veinticuatro meses serían un plazo mínimo. Como referencia para ajustar esos tiempos a la eficacia de su uso en las investigaciones, según los expertos policiales, la mayoría de las solicitudes de acceso se llevan a cabo sobre los datos generados en el año natural de la investigación o en los doce meses anteriores a esta.

Sexta. Garantías de seguridad de los datos. Una de las principales preocupaciones del Tribunal de Luxemburgo estaba relacionada, como así lo expresó en la Sentencia al *caso Digital Rights*, con el riesgo de abuso y de acceso o uso ilegal de los datos almacenados por los proveedores (apartados 66 a 68) al considerar que la Directiva no establecía medidas que aseguraran tal protección con un nivel adecuado y, además, se dejaba a cada proveedor la valoración de estas, en función de criterios económicos. Por tanto, es fundamental buscar alternativas que cumplan con los estándares requeridos por el Tribunal y contar con el criterio de los operadores y una adecuada evaluación de costes que habría que compensar de alguna forma (esta parte queda al margen de nuestro estudio, pero creemos que es necesario también explorar con el sector vías de apoyo y que no se limite a una imposición legal, sino como un enfoque que muestre también el beneficio en términos de reputación social corporativa).

Polo Roca[643] (2022; 127) concluye que, dado que la conservación de datos de las comunicaciones electrónicas compete al proceso penal, no es descabellado proponer que *"es Estado sufragase algunos de los gastos que las compañías de telecomunicaciones se vieron (y se ven) obligadas a hacer para incorporar la infraestructura necesaria para poder cumplir la obligación de conservar los datos de comunicaciones electrónicas"*. No estamos de acuerdo con esta propuesta, por cuanto no es el único ejemplo en el que se imponen obligaciones de colaboración del sector privado con el público que exige la adopción de medidas y, la asunción de costes, al sector privado, para contribuir a la investigación penal. Hemos citado el caso de la Directiva PNR, como podríamos poner otros también recientes -no mencionados en nuestra investigación, pero también actuales- como el control de sustancias susceptibles de ser usadas como precursores de explosivos, etcétera. Además, en este caso concreto, precisamente porque no hubo acuerdo al respecto durante la negociación de la Directiva invalidada, se otorgó a los proveedores de servicios la facultad de decidir cuáles eran las medidas idóneas para cumplir con lo recogido en la norma; y precisamente ha sido también *criticado* por el TJUE.

En este sentido, proponemos acudir igualmente a la Directiva PNR, que establece que se deberán utilizar técnicas de *"seudonimización"* que permitan despersonalizar los datos mediante su enmascaramiento; es decir, haciendo invisibles para un usuario aquellos datos que servirían para identificar al interesado/afectado.

Sin ánimo de extendernos en cuestiones técnicas, daremos algunas pinceladas sobre cómo se podría llevar a cabo esta acción, con la finalidad de justificar que es técnicamente posible y eficaz de cara a asegurar los datos y contribuir a garantizar la privacidad de los titulares de estos:

- El enmascaramiento de los datos que supone la *seudonimización*, según indica la Agencia ENISA[644] es una medida técnica aceptada como válida para la

[643] POLO ROCA, A., *La conservación de datos en el sector de las telecomunicaciones: un estudio sobre su regulación en la Unión Europea y su cabida en el Derecho de la Unión*, *Thomson Reuters, Aranzadi*, Pamplona, 2022, p. 127.

[644] ENISA (Agencia de la Unión Europea para la Ciberseguridad) es la agencia de la UE a la que se le ha encomendado la misión de velar por un alto nivel común de seguridad en toda Europa.

protección de los datos, que ha ganado protagonismo desde 2016, con la aprobación del Reglamento General de Protección de Datos, que lo menciona en reiteradas ocasiones. Como ha subrayado esta agencia, no existe una técnica de *seudonimización* que sirva para todo y es necesario un análisis detallado del caso en cuestión para definir la mejor opción posible[645]. No obstante, consideramos que es un punto de partida importante para intentar eliminar uno de los reparos más prematuros del TJUE que le llevó en 2014 a declarar la invalidez de la Directiva de 2006 y, en esta tarea, es fundamental contar con el criterio especializado del Supervisor Europeo de Protección de Datos y la participación también del sector de las telecomunicaciones, quienes propondrán las técnicas concretas más adecuadas al caso y la valoración de la medida en que garantizan que el enmascaramiento sea efectivo de cara a imposibilitar la asociación de los datos almacenados a individuos concretos.

Para nuestro objeto de estudio, los dos grandes grupos de datos habría que desagregar y almacenar de forma separada son los metadatos y la identificación de los usuarios que los han generado (los *propietarios* de esos datos), de forma tal que el acceso a unos u otros no permita conocer el contenido, por estar cifrados; ni relacionar un grupo con el otro. Lógicamente, por el hecho de tratarse de una técnica de *enmascaramiento,* debe ser posible establecer la relación entre ambos grupos mediante una autorización para ello y la disposición de la correspondiente *llave* de descifrado. Si no se pudiera realizar esta acción reversible, estaríamos en un supuesto distinto: la *anonimización*, que es irreversible y que impediría cumplir con el fin para el que se almacenan los datos.

Cuestión distinta, pero también necesaria, es determinar la forma de almacenamiento de estos, de forma separada, y el aseguramiento físico de las instalaciones, que creemos que deberían estar ubicadas en los Estados miembros.

[645] Para ampliar datos desde el punto de vista técnico de lo que es y los usos que se puede dar a la seudonimización, véase el informe de la Agencia ENISA: "Data pseudonymisation: advanced techniques and use cases. Technical análisis of cibersecurity measures in data protectin and privacy", January 2021, DOI 10.2824/860099, en https://www.enisa.europa,eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases consultado el 4 de octubre de 2022.

Esta es precisamente otra de las cautelas que planteó el Tribunal y, de hecho -especialmente de cara a la inclusión de las OTT- es una dificultad añadida, por cuanto algunos de los operadores de este tipo de servicios más novedosos tienen su ubicación geográfica fuera de la Unión Europea. En ese caso (como en el del PNR) se habrá de recurrir a acuerdos con terceros países. Somos conscientes de las dificultades que esta situación genera, aunque salvables, como han demostrado las negociaciones para la transferencia de datos PNR con EE. UU. o México, pero, sobre todo, con Canadá, que ha sido objeto del pronunciamiento más reciente del TJUE y que, aunque de forma lenta y con negociaciones difíciles (tanto entre la Comisión y los Estados miembros, como de la primera con Canadá), se está adaptando a esos criterios y se encuentra próximo a su aprobación.

- Para este caso, juega también un papel fundamental la autoridad independiente, ahora administrativa [consideramos que la autoridad judicial no debe participar en este proceso, como sí en el de la emisión de la orden de conservación y de acceso y tratamiento por las agencias encargadas de la aplicación de la ley]. La norma europea de nuevo cuño debería establecer a qué autoridad/es correspondería la labor de supervisión de los mecanismos y medidas que los proveedores deberían establecer para garantizar el proceso de *seudonimizacion* y custodia de los datos. Creemos adecuado valorar si el Supervisor Europeo de Protección de Datos pudiera ejercer esa labor a nivel europeo y coordinar también las acciones de las agencias nacionales de protección de datos.

- Una vez más nos fijamos en las soluciones adoptadas en el sistema PNR y, cuando los datos conservados hayan cumplido su función o hayan dejado de darse las condiciones que justificaron su almacenamiento, estos deberán ser borrados de forma irreversible[646]. Para el caso en que los datos hayan sido retenidos de forma general e indiferenciada, como los datos de identidad, o las IP de origen en el caso de la investigación de delitos graves [dejamos al margen

[646] El borrado es distinto de la *anonimización*, aunque ambas técnicas son irreversibles. La *anonimización* no está bajo el ámbito de aplicación del Reglamento General de Protección de Datos. Para profundizar en estos conceptos, vid. https://www.aepd.es/es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion, consultado el 29 de julio de 2021.

la conservación general e indiferenciada con fines de prevención de amenazas a la seguridad nacional] y no han sido solicitados y, en consecuencia, no han sido *cedidos* a los servicios policiales, también deberán ser borrados de forma irreversible al final del periodo de conservación previsto.

Séptima. Criterios orientativos sobre la conservación selectiva (geográficos, en base a grupos de personas, en base a la tasa/índice de delincuencia, a demandas sociales, etcétera).

Sirva como nota inicial el criterio de los expertos policiales, con el que estamos de acuerdo, acerca de que la conservación selectiva es insuficiente para desarrollar con la misma eficacia que antes el tipo de investigaciones que hemos relatado en otros capítulos precedentes; no obstante, es perentorio agudizar el ingenio y asumir que las reglas del juego han cambiado y obtener el máximo rendimiento de los *mimbres de los que disponemos*. El Tribunal sostuvo que es posible la conservación selectiva como medida preventiva para combatir la delincuencia y las amenazas graves para la seguridad pública siempre que se limite a lo estrictamente necesario con respecto a las categorías de datos que deben conservarse, los medios de comunicación afectados, las personas afectadas y el período de conservación adoptado. La conservación selectiva puede lograrse, en particular, ciñéndola a categorías o grupos de personas o a zonas geográficas específicas, sobre la base de factores objetivos y no discriminatorios.

En relación con las categorías de personas, el Tribunal indica[647] que la legislación sobre conservación selectiva puede dirigirse a personas cuyos datos de tráfico y localización puedan revelar un vínculo, al menos indirecto, con delitos graves, para contribuir de una u otra forma a la lucha contra la delincuencia grave. Las personas así seleccionadas podrán, en particular, ser aquéllas que hayan sido identificadas previamente en el curso de los procedimientos nacionales aplicables y sobre la base de pruebas objetivas, como una amenaza para la seguridad pública (o nacional) en el Estado miembro en cuestión. Después ha matizado su criterio, incluyendo también a las

[647] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartados 148 y 149.

víctimas y a las personas relacionadas con ella, como sospechosos o como testigos que puedan aportar elementos de investigación para el esclarecimiento de los hechos graves que originan la adopción de medidas.

Defiende Ortiz-Pradillo (2020; 19)[648] que, respecto del círculo de personas sobre el que establecer las medidas, como criterio subjetivo que es, resulta complejo de determinar con carácter preventivo sin -como recogía el Abogado General de la UE- correr el riesgo de *"instaurar un régimen de sospecha general sobre algunos segmentos de la población y catalogarse de discriminatoria, en función del algoritmo empleado"*[649], pues se trata de una conservación de datos para futuras investigaciones, si es que se producen, lo que, según Rodríguez Láinz (2107; 13), no se compadece con lo que el legislador quería regular a través del artículo 15, apartado1, de la Directiva de privacidad electrónica[650]. Ciertamente, estamos de acuerdo en la dificultad para determinar los criterios aplicables a la hora de establecer los grupos sobre los que se debería realizar una conservación selectiva y, más aún, qué grupos concretos cumplen con los criterios consensuados, ya que estos [los criterios] pueden variar de un Estado miembro a otro; algo que tendrá que valorar y ponderar el juez o la autoridad independiente que autorice las medidas. No cabe duda de que esta cuestión tampoco sería pacífica, como no lo fue la aprobación del texto final de la Directiva de conservación de datos, por lo que habrá que buscar el consenso de todos los actores implicados y hacer también pedagogía sobre su necesidad y su contribución a la seguridad de los ciudadanos. A modo de ejemplo, apuntándonos al ejercicio de aportación de ideas que han venido haciendo los magistrados europeos y por si pudiera servir de referencia para los decisores de las instituciones europeas, proponemos -entre otros- los siguientes grupos de personas: grupos conocidos de delincuencia organizada, individuos condenados por un delito grave, individuos que han sido objeto de una orden de interceptación legal; individuos de los que las autoridades tienen razones para creer

[648] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones penales…", op. cit.*, p. 19.

[649] Conclusiones del Abogado General de la Unión en el Caso C-520/18, apartado 88.

[650] RODRIGUEZ LÁINZ, J.L., *"La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones*", Diario La Ley, nº. 8901, de 16 de enero de 2017, p. 13.

que tienen un vínculo con la delincuencia grave; individuos que figuran en un lista de vigilancia[651]; etcétera.

El Profesor Ortiz-Pradillo (2020; 19)[652] observa también que la determinación de grupos mediante la exclusión de algunos de ellos en base a secreto profesional o a determinadas prerrogativas de las que estos puedan gozar facilitaría la labor; no obstante, aun así, aunque sería más fácil acordar a qué grupos de personas nos estamos refiriendo en este caso, creemos que reduciría escasamente el trabajo de agrupamiento. Sí nos parece más interesante explorar la idea que también suscita acerca de poner el acento en el sujeto pasivo de la comunicación (de quien recibe una conexión de determinadas personas o entidades) o de un determinado tipo de usuarios de un medio de comunicación concreto o de un dispositivo particular. A priori, podrían servir de criterios, también subjetivos, para un determinado grupo de personas o colectivos sobre los que plantear una conservación selectiva. Pero habrá otros sobre los estudiar igualmente su viabilidad, para incorporarlos a la nueva norma europea de conservación de datos que proponemos.

En resumen, de los criterios que ha indicado el propio Tribunal, este nos parece el menos útil a efectos prácticos, al menos respecto de la determinación de un colectivo amplio, puesto que suscitará muchas dudas a quien tenga que valorar la eventual autorización, por la colisión con otro tipo de derechos de los colectivos o grupos concretos elegidos en un momento dado. Nos parece más apropiado para decisiones sobre grupos reducidos de personas que se centren en un determinado sospechoso o su víctima y los cercanos/allegados a uno u otro; sin embargo, este tipo de decisiones sobre grupos tan pequeños creemos que no debería considerarse ni siquiera incluida en el ámbito concreto de lo que la norma europea debería regular. Queremos decir que una investigación sobre unas 15 o 20 personas (por poner un ejemplo aleatorio) no creemos que sea un supuesto como los que la Directiva de 2006 quería regular, ni la nueva norma debería tampoco hacerlo. Aunque en puridad sea así, a nuestro entender se asemeja más a una autorización como la que un juez otorga para otros medios de

[651] *"Watchlist"* en inglés.

[652] ORTIZ-PRADILLO, J.C., *"Europa: auge y caída de las investigaciones penales…", op. cit.*, p. 19.

investigación: colocar un dispositivo de vigilancia a unos sospechosos o una entrada y registro en un *puñado* de domicilios.

Respecto de la selección geográfica, se podrán incluir zonas en las que[653] las autoridades nacionales consideren, basándose también en factores objetivos y no discriminatorios, que existe una situación caracterizada por un alto riesgo de preparación o comisión de delitos graves. Estas pueden afectar a lugares con una alta incidencia de delitos graves (la referencia expresa a la tasa de delincuencia la incluyó el Tribunal en las sentencias más recientes, consideramos que en un intento por *auxiliar* a las autoridades públicas en la fijación de criterios selectivos, tras la reiterada presentación de cuestiones prejudiciales sobre las asuntos recurrentes); lugares especialmente vulnerables a la comisión de delitos graves, como barrios acomodados, lugares de culto, escuelas, lugares culturales y deportivos, de reuniones políticas y cumbres internacionales, parlamentos, tribunales, centros comerciales, aeropuertos y otras infraestructuras críticas, estaciones o zonas de peaje, etcétera. Este criterio, basado en el establecimiento de un área espacial sobre el que prever la conservación de datos, nos parece más objetivo -o menos subjetivo, si se quiere- que el basado en grupos de personas, aunque también puede verse afectado por sospechas de estigmatización de determinados colectivos que habitualmente viven en zonas deprimidas donde se concentra un mayor índice de comisión de delitos graves. En cualquier caso, nos parece más adecuado que el basado en grupos de personas, aunque exigirá una revisión permanente del mantenimiento de las circunstancias iniciales o su evolución favorable a la prórroga. Aun así, somos conscientes que determinados delitos que se cometen exclusiva o principalmente a través de Internet -muchos de los que requieren del uso de estos datos para su investigación-, no pueden asignarse fácilmente a una zona geográfica concreta, ni a nivel nacional ni menos aún internacional.

Pero, al margen de las dificultades para delimitar grupos de personas o áreas geográficas [máxime cuando en el momento en que se necesita acceder a la información normalmente no se pueden establecer todavía esos criterios y muy probablemente

[653] Sentencia TJUE (Gran Sala), de 6 de octubre de 2020, caso *La Quadrature du Net*, apartado 150.

obligará a solicitar a la autoridad habilitante la modificación de la medida, normalmente para ampliar las zonas de interés o las personas bajo sospecha o relacionadas, y añadirá indefectiblemente una carga de trabajo importante que retrasará la decisión de autorización y perjudicará en determinadas ocasiones la oportunidad de la medida], surgirán problemas técnicos añadidos, relacionados con la propia inexistencia de fronteras en el ciberespacio, que mencionábamos antes, y la casi imposibilidad de fijar límites, especialmente en aquellos delitos que se cometen exclusivamente a través de los sistemas de comunicación electrónica, que no tienen una jurisdicción definida o que afecta a varias y alejadas áreas geográficas.

Tanto en un caso como en el otro, la labor de los investigadores de argumentación y precisión de los hechos y el trabajo previo que también tendrán que realizar para acotar a personas o colectivos y lugares a los que aplicar las medidas, se convierte en fundamental, puesto que ante estos criterios que parecen muy acotados, pero que ofrecen una casuística inmensa, es difícil llegar a un acuerdo sobre un listado cerrado de supuestos que satisfaga a todos los Estados miembros; y tampoco nos parece operativo que la nueva norma descienda a ese nivel de detalle que podría encorsetar la actuación policial y dificultar la modificación del listado, cuando sea necesario. Creemos que no es una labor tan necesaria ni *fácil* como la enumeración de los delitos graves sobre los que operar [vimos que en la Directiva PNR se consiguió] o las categorías de datos imprescindibles o prescindibles, sobre los que sí vemos oportuno que los expertos y decisores a nivel de las instituciones europeas deban trabajar como parte de la evaluación de impacto previa a la presentación de una nueva propuesta normativa. En esta labor, aunque a estas alturas es innecesario mencionarlo, por obvio, se deberán respetar los derechos y libertades fundamentales de los afectados y, de forma particular, lo recogido en el artículo 21 de la Carta de los Derechos Fundamentales de la Unión Europea, relativo a la no discriminación de las personas[654].

[654] Artículo 21CFUE: *"1. Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual. 2. Se prohíbe toda discriminación por razón de nacionalidad en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea y del Tratado de la Unión Europea y sin perjuicio de las disposiciones particulares de dichos Tratados"*.

Octava. Criterios específicos para una conservación rápida *o quick freeze*.

La principal característica diferenciadora de este supuesto respecto de la conservación selectiva está en que la solicitud se lleva a cabo una vez que se ha conocido un hecho u hechos concretos sobre los que se ha iniciado o se va a iniciar una investigación; es decir, es una actividad puramente reactiva y no preventiva. La rapidez se exige por la inmediatez para asegurar la información que aportan los posibles metadatos generados por las comunicaciones electrónicas de los usuarios/abonados, a partir del momento en el que se ordena su conservación. En cualquier caso, el histórico de los datos anteriores a la autorización y aplicación efectiva de la medida no estará disponible. En consecuencia, se perderán datos muy importantes anteriores al momento de conocimiento de los hechos. La conservación selectiva tiene una función mayormente preventiva, ante supuestos concretos o desconocidos pero previsibles, en base a determinados criterios que hemos reflejado en la consideración séptima.

En este caso, creemos que se podría solicitar el acceso a los datos históricos que el proveedor de servicios afectado conserva para sus fines comerciales y de negocio (siempre que en ese momento sigan estando disponibles), por lo que se podría contar con más información que, aunque pueda ayudar en determinados supuestos, no satisfará las necesidades de los investigadores. El Tribunal no deja claro si se podría o no acceder a esos datos anteriores a la medida, aunque entendemos que no se opone, cuando lo redacta con el siguiente tenor: *"el recurso a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida (quick freeze) de los datos de tráfico y de localización de que dispongan estos proveedores de servicios,…"*[655]

El elemento común entre ambas situaciones está en la necesidad de obtener una orden de conservación por parte de la autoridad judicial o administrativa correspondiente.

[655] Sentencia TJUE, de 20 de septiembre de 2022, *Caso SpaceNet AG* C-793/19 y C-794/19, apartado 75.

Respecto del establecimiento de medidas de seguridad sobre esos datos, o sobre el procedimiento para su remisión a las autoridades requirentes o su borrado posterior, creemos que no deben establecerse criterios diferentes a los previstos para la conservación selectiva.

Novena. Diferenciación entre tipo de datos.

El Tribunal ha diferenciado entre categorías de datos, otorgando un menor nivel de injerencia en los derechos fundamentales afectados para algunos de ellos y, en consecuencia, permitiendo acciones más amplias y sostenidas en el tiempo respecto de su conservación y acceso. Nos referimos aquí expresamente a los datos de abonado/suscriptor, sobre los que se permite una conservación generalizada e indiferenciada, cumpliendo los mismos criterios que hemos venido analizando para el resto de las situaciones y categorías de datos. Por tanto, la norma europea deberá tener en cuenta también esta circunstancia, que afectará no solo a la prerrogativa de conservación en toda su extensión material, sino también al tiempo de conservación, que entendemos que podrá ser más amplio (ya nos hemos referido en la consideración cuarta de forma indirecta a la diferenciación en cuanto a la categoría de datos).

Décima. Obligación de información a las personas afectadas.

Por contradictorio que pueda parecer, respecto de la debida reserva que rodea a las investigaciones penales (máxime cuando se realizan sobre la comisión de delitos graves), la norma europea deberá regular los supuestos en los que se limitará la obligación que recoge la normativa europea de protección de datos y la doctrina del TJUE de informar a los sujetos afectados por la injerencia en su privacidad y protección de los datos personales. Puesto que la regla general es el deber de información, habrá de debatirse entre los expertos y decisores europeos, y reflejar en el articulado, aquellos supuestos concretos que eximirán a los investigadores de realizar tal comunicación o quizás sirva también su dilación en el tiempo a momentos en los que la comunicación no perjudique las pesquisas. En ocasiones, será simplemente imposible informar a todos y cada uno de los afectados, como también lo será decidir a quiénes se informa y a quiénes no, por imposibilidad material y temporal para hacerlo y, aunque esta

circunstancia no justifica la inacción, por la indisponibilidad de recursos humanos para ello.

Al margen de lo tratado en nuestra tesis, se propone explorar la opción de que los suscriptores de servicios como los que venimos analizando, firmen en sus contratos de adhesión (o en el consentimiento que se otorga al descargar una aplicación en un Smartphone) una cláusula por la que aceptan transferir los datos de abonado/suscripción, e incluso los que se puedan generar a través de los servicios que incluye el contrato, a las agencias encargadas de la aplicación de la ley, a los efectos de la prevención e investigación, persecución y enjuiciamiento de delitos graves; informando también de los derechos ARCO más portabilidad y olvido que le asisten, en base a lo recogido en el Reglamento Europeo de Protección de Datos. Creemos que sería conveniente analizar esta posibilidad, con sus pros y sus contras, pero lo dejaremos para un estudio aparte, por nuestra parte o por quien pueda considerarlo de interés tras la lectura de este trabajo, si es que no se está ya abordando.

Undécima. Ámbito de aplicación de la norma.

Una cuestión igualmente importante es la determinación del ámbito de aplicación de la futura norma respecto de los proveedores de servicios afectados, no ya en cuanto al tipo de servicios prestados (que hemos analizado antes) sino de la ubicación de la empresa o el área geográfica de prestación de sus servicios. Puesto que la norma afectará a la Unión Europea, será necesario explorar, de entre las opciones disponibles, y de forma alineada con lo recogido en el próximo Reglamento de privacidad electrónica, si se aplica solo a las empresas europeas del sector o se extiende también a las empresas extranjeras que prestan servicio en la Unión Europea. La segunda opción nos parece más apropiada en términos de eficacia de las medidas y teniendo en cuenta que muchas de ellas (la mayoría de las OTT) tienen sus sedes centrales en terceros países, por lo que, de no ser así, quedaría fuera del alcance de la nueva norma una parte muy importante y sustancial del nuevo esquema de las nuevas tecnologías y de la comunicación, actuales y futuras. Los expertos deberán debatir sobre esta cuestión, partiendo de las discusiones previas y lo regulado para el sistema PNR, en

el futuro sistema europeo de acceso a la prueba electrónica[656] [no hemos tratado este paquete legislativo en nuestra investigación, pero tiene relación con la materia de nuestro interés] o en los diálogos con determinadas empresas tecnológicas para solicitar su colaboración en la retirada de contenidos en línea de carácter terrorista o que incitan a la comisión de atentados o al proselitismo.

En las discusiones previas a la presentación del borrador de nueva norma, no se puede dejar de lado tampoco la reflexión sobre si debe hacer mención de los mecanismos de cooperación que serán necesarios de forma frecuente, teniendo en cuenta el carácter transfronterizo de la mayoría de estas investigaciones: OEI, OED, acuerdos con terceros países, etcétera.

Decimosegunda. Acceso a los datos conservados.

El acceso a los datos conservados es la segunda cuestión principal del sistema, aunque no se la mencione tan frecuentemente como al almacenamiento de los datos. Lógicamente, la finalidad de la retención es que los datos estén disponibles para ser puestos a disposición de las autoridades.

Esta parte, pese a su importancia, debido a que las decisiones y las acciones quedan sometidas al criterio de las autoridades nacionales, a nuestro entender, permiten solo el establecimiento en la norma europea de ciertos requisitos mínimos que traten de armonizar la actuación de los Estados miembros, siempre bajo parámetros procesales nacionales; eso sí, dentro del marco establecido por el Tribunal y con respeto a los derechos y libertades fundamentales que recoge la Carta. El resultado de la valoración

[656] La propuesta de la Comisión sobre el establecimiento de un marco europeo común para el acceso transfronterizo a prueba electrónica en el ámbito de los procedimientos penales está todavía en fase de negociación interinstitucional. Consta de dos propuestas de reglamento: i) propuesta de reglamento del Parlamento y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a los efectos de enjuiciamiento penal COM (2018) 0108 (COD), para profundizar, vid. https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0006.02/DOC_2&format=PDF y ii) propuesta de Directiva del Parlamento Europeo y del Consejo estableciendo reglas armonizadas sobre el nombramiento de representantes legales para la recogida de pruebas en procedimientos.

de la autoridad competente habilitante será la autorización o denegación, tanto para la solicitud inicial, como para su ampliación y prórroga, si fuera necesaria.

Recordemos que el Tribunal es contundente en sus últimas sentencias a la hora de afirmar que no se puede salvar la conservación injustificada mediante garantías reforzadas para el acceso. Por tanto, se obliga a las autoridades judiciales y administrativas habilitadas a valorar si la conservación es necesaria y proporcionada, antes de autorizar o no el acceso y tratamiento.

La norma deberá también fijar los plazos a partir de los cuales deberá borrarse la información accedida y tratada, sujeto a consideraciones también por parte de la autoridad judicial, y el procedimiento para asegurar que desaparecen definitivamente. Como en la Directiva PNR, se debería estudiar y discutir la posibilidad de un estadio intermedio de enmascaramiento [nos referimos aquí a los datos que ya están a disposición de los servicios policiales] previo a la eliminación definitiva. En esta discusión, pueden ayudar los debates y el texto final de la Directiva PNR. Se debería también discutir acerca del tiempo en el que los servicios policiales pueden acceder a los datos que se les ha cedido, aunque este plazo estará limitado en la autorización judicial o de la autoridad administrativa, quienes entendemos que otorgarán la prerrogativa sobre el manejo de los datos durante un espacio temporal limitado, a partir del cual tendrán que decidir sobre la prórroga o cancelación de la medida, como se hace habitualmente con otras medidas restrictivas de derechos como la intervención telefónica.

Hay otro tipo de consideraciones que entendemos que corresponden a materias de índole nacional, pero sobre las que se podría incluir alguna referencia general (o bien en los considerandos de la norma; en la parte programática). Nos referimos al establecimiento de salvaguardas en la gestión interna de las unidades de investigación y los servicios policiales sobre cómo asegurar que el acceso y tratamiento de los datos están restringidos a los miembros de la unidad que se encarga de la investigación y no otros; que se custodian adecuadamente y que no se pone en peligro la privacidad de los

ciudadanos afectados. En cualquier caso, este tipo de actuaciones están sometidos a controles tanto internos, por parte de los propios servicios policiales; como de las agencias de protección de datos nacionales.

El Tribunal acepta que, para una determinada categoría de datos, como son los datos de identidad o de suscripción, el acceso pueda ser autorizado por alguna autoridad diferente a las anteriores (por ejemplo, la Policía judicial), al considerar que la injerencia en los derechos de los titulares de los datos no es grave. Deberá regularse también claramente en la norma europea.

2.2.Otras particularidades relacionadas

Decimotercera. Ya nos hemos referido a este aspecto en varias ocasiones, pero queremos reflejarlo aquí de forma específica para resaltar la importancia de contar con el sector de las telecomunicaciones y la sociedad de la información, no como meros espectadores a los que pedir opinión y cumplir así un trámite que ni siquiera es preceptivo, sino para involucrarlos desde el principio y en toda la cadena de valor, explicando la importancia de su asesoramiento y apoyo más allá de las obligaciones legales que se les puedan imponer y haciéndoles ver su contribución a la protección de los ciudadanos y los beneficios que en términos de reputación social corporativa tendrá para las empresas.

Esta colaboración es más importante si cabe a la hora de fijar la concepción de los nuevos desarrollos tecnológicos, los que están en fase de desarrollo y los que están por venir (5G, IoT, técnicas de cifrado de la comunicación, IA, etcétera), dado que es un sector en continua evolución y muy complejo. Es habitual que no se tengan en cuenta las necesidades de las agencias encargadas de la aplicación de la ley en esos procesos. En este caso, el acercamiento debe ser desde el ámbito de los servicios policiales y los responsables en la Unión Europea de esta materia (como puede ser EUROPOL, ENISA, etcétera) hacia las empresas tecnológicas, tanto europeas como internacionales, dado que el interés parte de ellas más que de las propias empresas del sector.

Decimocuarta. Autoridades competentes para el acceso y tratamiento de los datos.

Otra cuestión que no está claramente definida y que presenta excesiva *variedad* entre los Estados miembros, tanto por la diferencia de competencias y dependencias de los distintos actores (policiales, agentes de fronteras, servicios de inteligencia, organizaciones puramente administrativas, etcétera) que deberán acceder a la información y tratarla para la prevención, investigación, persecución y enjuiciamiento de delitos graves; como por la dependencia y organización jerárquica a nivel ministerial, es la determinación de quiénes, en cumplimiento de sus deberes legítimos, podrán acceder a la información y quiénes no. En este sentido, consideramos que la norma europea debe establecer alguna definición general que acote, en base a las funciones propias de quienes deberían estar habilitados para tal fin, el concepto genérico de *autoridades competentes* a los efectos de la norma, con el ánimo principal de orientar a los Estados miembros. Es cierto que la responsabilidad última recaerá sobre los jueces y/o autoridades administrativas con competencia para autorizar el acceso y tratamiento de los datos, a la hora de determinar estas autoridades en cada uno de los países.

Lo anterior no es más que una recomendación, pero creemos que es oportuna, ya que hemos visto casos concretos parecidos que han sido puestos en conocimiento del Tribunal y que ha derivado en pronunciamientos aclaratorios. Uno de ellos, según nuestro criterio, estaba ya claro antes de conocer el fallo del TJUE: el hecho de que un miembro de la Policía, por mucho que cuente con una unidad específica para ello y él no forme parte de las investigaciones, no ofrece la neutralidad e independencia suficientes como para autorizar o no la injerencia en derechos fundamentales de los ciudadanos. El otro, nos parecía menos evidente, pero también se aclaró en la sentencia al Caso Ministerio Fiscal, en la que se pone en entredicho la independencia respecto de la labor investigativa de los fiscales [no en España, pero sí en la mayoría de los países, al ser quienes dirigen las investigaciones penales].

Y relacionado con lo anterior, creemos que, aunque no en el articulado de la norma, pero sí mediante otro tipo de iniciativas, en el marco de las reuniones del Comité de Coordinación en el ámbito de la cooperación policial y judicial en materia penal

(CATS, por sus siglas en inglés)[657], se debería abordar la puesta en común de orientaciones/guías para los jueces y autoridades administrativas facultadas para autorizar la conservación y el acceso a los metadatos, a la hora de homogeneizar la prueba de necesidad y proporcionalidad que deberán efectuar (como lo hacen ya para otros ámbitos) y unificar criterios en la medida en que los regímenes jurídicos propios de cada país lo permitan, pero sí al menos en la interpretación de la doctrina del Tribunal europeo de Justicia.

Por último, respecto del acceso a los datos conservados en un Estado miembro distinto a aquel en el que se está llevando a cabo la investigación, se deberá dejar a un desarrollo posterior, mencionado en la norma, el establecimiento de mecanismos para intercambiar la información pertinente entre autoridades judiciales nacionales de los Estados miembros. En ese sentido, debería conectarse la norma de conservación de datos con el marco europeo de acceso transfronterizo a prueba electrónica que mencionábamos anteriormente y que está siendo objeto de aprobación todavía hoy, después de varios años de debate en el seno de las instituciones europeas. Para la solicitud de acceso a datos almacenados en terceros países, habrá que recurrir a otras formas de cooperación que hemos apuntado en párrafos procedentes; también eficaces, pero más lentos y administrativamente más tediosos.

Somos conscientes de que, incluso si se aceptara poner en marcha las medidas que aquí proponemos, y aquellas otras que puedan complementar y mejorar estas, serían necesarios todavía algunos años hasta que la nueva norma viera la luz. En cualquier caso, estamos convencidos de que no se puede perder más tiempo para comenzar el recorrido con una propuesta legislativa de la Comisión sobre la que comenzar a negociar y consensuar.

[657] Coordinating Committee in police and judicial cooperation in criminal matters (CATS). Para profundizar, vid. https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/coordinating-committee-area-police-judicial-cooperation-criminal-matters/

CAPÍTULO X. CONCLUSIONES

Llegamos al final de nuestra investigación y es el momento de extraer conclusiones. Al contrario de lo que pudiera parecer en las primeras pinas, o de la propia elección de los capítulos y las temáticas tratadas, lo que presentamos a continuación no son conclusiones preconcebidas de antemano, sino consecuencia del estudio y tratamiento de la información que hemos manejado y de los caminos por los que nos ha llevado. De hecho, a medida que esta avanzaba, hemos cambiado incluso nuestro pensamiento inicial respecto de cuestiones sobre las que los expertos tienen un criterio más o menos consolidado.

Las recapitulaciones que presentamos a continuación no siguen un orden temático ni por capítulos, sino que están agrupadas conceptualmente, por cuanto la interrelación entre las materias abordadas en cada uno de los apartados de la tesis es lo que permite contextualizar mejor el problema de estudio y sus consecuencias. De alguna forma, las propuestas que ofrecemos en el capítulo anterior (capítulo IX) ya dejan entrever algunas de las consideraciones que haremos, por lo que necesariamente repetiremos algunos de los argumentos previamente presentados. Empero, creemos que merecen ser detallados también en las conclusiones.

Primera. La principal conclusión a la que hemos llegado [y por ello la posicionamos en primer lugar] tiene que ver con un concepto poco científico, pero determinante en todos los aspectos de la vida: voluntad y determinación; en este caso, para asumir una realidad y vencer el *sesgo del statu quo*. Ocho años después de la primera sentencia, tras la invalidación de la Directiva 2006/24/CE y la confirmación por el TJUE de su doctrina inicial -al margen de la leve modulación de su posición, con introducción de criterios y casuística concretos- es necesario asumir que la situación no volverá a ser como en 2006, en la medida en la que ya no se aprobará una conservación generalizada e indiferenciada de todos los datos de todas las comunicaciones electrónicas de todos los ciudadanos europeos[658]; y es perentorio buscar alternativas para obtener el mayor beneficio de la nueva realidad. Como indica el propio Tribunal,

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

corresponde a los Estados miembros determinar las opciones y posibilidades que permitan luchar de forma eficaz contra la delincuencia grave y otras amenazas, de acuerdo con la excepción a la normativa europea vigente sobre privacidad en las comunicaciones electrónicas. Creemos haber encontrado algunas opciones y alternativas, al menos como punto de partida sobre el que construir un nuevo sistema de conservación de datos de las comunicaciones electrónicas en la Unión Europea.

Segunda. Alargar la situación actual supone mermar las posibilidades de actuación de los servicios policiales y otras autoridades competentes en la defensa de los derechos de los ciudadanos y extender sus efectos adversos a procesos judiciales en curso en los que se ha admitido la validez de las pruebas obtenidas en base a las normativas nacionales aun en vigor. No hay actualmente ningún indicio, de acuerdo con las sentencias en la materia, de que el Alto Tribunal vaya a modificar de forma sustancial su doctrina. Lo más que hemos advertido es un intento por cerrar el asunto causando un impacto moderado y proporcionado en la relación entre instituciones, en la clásica disputa entre estas por defender sus respectivos roles en la construcción europea, llegando incluso a lo que Polo Roca[659] refleja de la siguiente manera -y estamos de acuerdo- que *"el cuerpo de la sentencia [La Quadrature du Net y otros] es casi una directiva, a falta de un articulado"*. Posteriormente a esta afirmación, el Tribunal ha precisado aún más otros aspectos que hemos analizado en la sentencia más reciente, de septiembre de 2022, de forma que nos hacemos la misma pregunta que el autor: *"¿podría ello llegar a plantear una situación de actividad ultra vires del Tribunal, sobrepasando el marco de actuación de los tratados?*

Tercera. El debate entre Libertad y Seguridad es clásico, como lo es también el que no se haya alcanzado consenso entre los expertos respecto de dónde situar el punto de equilibrio. La Unión Europea, a través de sus instituciones -quizás consciente de ello, dejó fuera de su ámbito competencial la adopción de medidas legislativas sobre seguridad nacional y otras materias de derecho penal y de cooperación policial y judicial, de forma que fueran los Estados miembros quienes acordaran mecanismos de cooperación, incluso reforzada, en el caso de que no hubiera consenso entre todos. Este

[659] POLO ROCA, A., *"La conservación de datos en el sector de las…", op. cit.*, p. 124.

principio general se ha visto matizado con el paso del tiempo y, sobre todo, tras el desmoronamiento de la estructura de pilares anterior al Tratado de Lisboa, que ha difuminado los límites de las competencias antes atribuidas a cada institución y ha abierto el campo de acción del Tribunal de Justicia europeo, que se pronuncia cada vez más sobre materias que antes eran objeto de tratamiento por los tribunales nacionales.

Respecto de la cooperación reforzada a la que nos referíamos en el párrafo anterior, aunque no es la opción más deseada, no cabe descartarla como alternativa ante la falta de acuerdo unánime de los Estados miembros para aprobar una nueva directiva que regule la conservación de datos. En un caso diferente al de la materia de nuestra tesis, pero igualmente relevante respecto de la contribución a la adopción de iniciativas en el ámbito de cooperación judicial (y policial), se recurrió a las posibilidades que ofrece el artículo 76 del TFUE, que permite que determinadas medidas puedan sean adoptadas *"por iniciativa de la cuarta parte de los Estados miembros"*. Nos referimos a la Fiscalía Europea[660]. La Comisión presentó una propuesta de reglamento de creación de esta institución en 2013 y, tras varios años de negociación y falta de la unanimidad requerida entre los Estados miembros, se decidió continuar por medio de esta forma de cooperación y concluyó con la aprobación de la fiscalía. Actualmente 22 Estados miembros forman parte de ella.

Cuarta. El debate entre estos dos derechos o grupos de derechos es recurrente y suele emerger cada vez que se produce algún lamentable acontecimiento o fenómeno que pone en jaque la seguridad de la Unión y sus ciudadanos. No obstante, son irreconciliables las posiciones de quienes creen que se debe hacer más en la adopción de medidas para garantizar la Seguridad, achacando que no se produzca un mayor avance al otro grupo (quienes tampoco quedan satisfechos, aunque se establezcan garantías de respeto de los derechos y libertades fundamentales de los ciudadanos). Consideramos que las amenazas a la seguridad de la Unión y sus Estados miembros es real y actual, y que no se pueden descartar situaciones que ya considerábamos superadas; lo que obliga

[660] La Fiscalía Europea o *European Public Prosecutor Office* (EPPO, por sus siglas en inglés) tiene competencia para investigar los delitos contra el presupuesto de la UE y ejercer la acción penal contra sus autores y llevarlos a juicio. Es un órgano independiente que empezó a funcionar el 1 de junio de 2021. Para profundizar, vid. https://www.consilium.europa.eu/es/policies/eppo/

a estar preparados. La actual invasión de Ucrania [como ocurrió también con la reciente pandemia del COVID-19, salvando las distancias] nos enseña que, si no se han adoptado medidas de protección y reacción, si no se está preparado para este tipo de situaciones, lleva mucho tiempo iniciar un proceso de decisión, discusión y aprobación cuando la necesidad se transforma en urgencia (además del considerable incremento de los recursos económicos requeridos para ello, que quedan al margen de este trabajo, pero que, si bien siempre ha sido obligatorio tenerlos en cuenta en la adopción de medidas, ahora debería serlo más si cabe).

No estamos de acuerdo con conceptos que hemos recogido y que se utilizan fundamentalmente en el ámbito académico como *securitización o tecnovigilancia*, para referirse al incremento de medidas, en este caso en el ámbito europeo, para extender el control de las agencias encargadas de la aplicación de la ley sobre los ciudadanos. Hemos dejado constancia de que esas acciones nacen de una necesidad identificada por las instituciones europeas y los decisores políticos de los Estados miembros y, después de un proceso de reflexión, análisis, discusión y toma de decisiones con amplio apoyo, se aprueban, casi nunca con unanimidad, pero con un consenso suficiente como para otorgarles legitimidad. Los servicios policiales y otras agencias encargadas de la aplicación de la ley se convierten posteriormente en los garantes de su aplicación y, ante situaciones de mala praxis o deficiente ejecución -escasas, aunque no totalmente descartables-, existen mecanismos de control, asunción de responsabilidades y reparación del daño causado.

En el caso de la Directiva 2006/24/CE, no hubo ánimo de adoptar medidas que conculcaran gravemente los derechos fundamentales de los ciudadanos europeos, pero sí hubo quizás improvisación, precisamente porque se reaccionó ante hechos como los que hemos relatado (atentados terroristas en suelo europeo y cambios geopolíticos que, unidos a una deficiente gestión de las fronteras exteriores de la Unión Europea, mostraron las vulnerabilidades de la seguridad europea) y había gran presión en los Estados miembros (no solo en aquellos que habían sufrido atentados recientes o no muy alejados en el tiempo, como España, Francia o Reino Unido) para adoptar acciones. Si se hubiera actuado con mayor antelación, con menos presión de tiempo, se habrían

podido atender las demandas y sugerencias de los órganos consultivos y otros actores involucrados en la Directiva y probablemente no se habría llegado al pronunciamiento del Tribunal europeo de 2014 y a los sucesivos que conocemos hasta hoy (octubre de 2022).

Quinta. La protección de los derechos y libertades fundamentales de los ciudadanos europeos ha ido evolucionando a lo largo del tiempo, como en otras partes del mundo, fruto de la integración europea y de la configuración de un acervo comunitario en materia de derechos fundamentales y humanos, pero también de la consolidación del Tribunal de Justicia de la Unión Europea como *tribunal constitucional* europeo, no solo para las materias comunitarias, sino también, con el paso del tiempo, para aquellas otras no compartidas pero a las que se han de aplicar igualmente la Carta de los Derechos Fundamentales de la Unión Europea. De esta forma, se ha conseguido armonizar en cierto modo la aplicación del derecho en determinados ámbitos fundamentales y también en materia de seguridad e investigación penal. De esa forma, se garantiza que determinados ámbitos relacionados con la Seguridad se aborden a nivel europeo con mayor determinación. Aplaudimos esa evolución, habida cuenta de que los retos actuales cada vez se pueden abordar en menor medida desde una perspectiva puramente nacional.

Además, la visión europea respecto del respeto de los derechos fundamentales está permitiendo también avanzar por la vía de los hechos, aunque sea con reticencias, hacia una mayor integración europea en cuestiones del Espacio de Libertad, Seguridad y Justicia. Como contrapartida, los parlamentos y tribunales nacionales se ven constreñidos en mayor medida por la actuación del Tribunal de Luxemburgo, limitando su capacidad de acción y provocando dilaciones en procesos judiciales (o administrativos) nacionales, amén de discursos (aunque puntuales) en algunos Estados miembros abogando por la *insumisión* ante determinados pronunciamientos del TJUE.

Sexta. No solo en Europa (aunque también), los avances en cuanto a la protección de la privacidad y de los datos de carácter personal se han producido en gran

medida debido a la propia evolución de las tecnologías de la información y las comunicaciones. Esta situación no solo ha servido a los ciudadanos en sus relaciones personales y profesionales a través de estos medios de comunicación, sino que ha permitido también a los delincuentes valerse de las medidas de protección en la comisión de sus acciones delictivas. En cambio, no se ha producido un avance en la misma medida y al mismo ritmo para permitir a las agencias encargadas de la aplicación de la ley disponer también de recursos legales y tecnológicos para desarrollar su labor de garantes de la Seguridad en un nuevo espacio, no físico y en cierta medida todavía desconocido y muy cambiante: *el virtual o de las ondas*, por el que deben *patrullar* y realizar investigaciones de tipo penal. En cierto modo, no se ha dotado de recursos que permitan desarrollar eficazmente la misma labor que a diario se lleva a cabo en pueblos y ciudades para garantizar la seguridad de los ciudadanos, pero ahora en un entorno virtual.

Las medidas hacia un nuevo sistema de conservación de metadatos de las comunicaciones electrónicas deben inexorablemente partir del consenso entre los colegisladores en las instituciones europeas (Consejo de la UE y Parlamento Europeo), tras una propuesta legislativa de la Comisión que palíe los errores de la Directiva de 2006 y con la participación de todos los actores implicados (también el sector profesional afectado y la sociedad civil). De acuerdo con Castellanos Claramunt (2022; 116)[661], la participación consigue que los ciudadanos se involucren en el espacio público y, para ello, se ha de aportar información clara y veraz.

Mantener soluciones nacionales, en un entorno global de supresión de fronteras y, al mismo tiempo, de interdependencia entre lo físico y lo lógico o digital; entre ciudadanos de un mismo país y, al mismo tiempo, con los de otras partes del mundo; es del todo inoperativo e ineficiente. Ese fue uno argumentos esgrimidos en la Directiva anterior, y no se puede retornar ahora a soluciones nacionales.

[661] CASTELLANOS CLARAMUNT, J., *"Transparencia y participación ciudadana…"*, op. cit. 116.

Séptima. Las leyes nacionales de transposición de la Directiva 2006/24/CE, si bien no pierden su vigencia de forma automática, no *pueden* seguir aplicándose ya a la luz de las reiteradas sentencias del TJUE. El principio general ha sido matizado por el Tribunal en las últimas sentencias, al considerar que, aunque corresponde al derecho nacional la admisibilidad y valoración de las pruebas, los tribunales nacionales deben dejar de lado aquellas obtenidas mediante una conservación general e indiferenciada en contravención de la legislación de la Unión.

Si, a pesar de este criterio, todavía se continúa instando al Alto Tribunal para que se pronuncie sobre cuestiones concretas de legislaciones nacionales, existe un riesgo cierto de que se dilate aún más la toma de decisiones sobre la adopción de un nuevo marco europeo de conservación de datos. Es poco probable que se produzca un cambio de criterio y, al mismo tiempo, se pueden *tirar por tierra* muchos procesos judiciales que juzgan delitos muy graves y conductas socialmente muy alarmantes y repugnantes, o incluso la revisión de condenas anteriores y la indemnización de las víctimas. Además, consideramos que se está trasladando a los proveedores de servicios una responsabilidad de conservación que les genera inseguridad jurídica y eventuales sanciones administrativas y/o penales, tanto si prosiguen con el sistema de almacenamiento de datos como si no lo hacen.

Octava. Sin cuestionar la obligación de realizar un análisis de necesidad y proporcionalidad a la hora de evaluar la colisión entre derechos fundamentales, consideramos que corresponde a los poderes públicos *esforzarse* más a la hora de buscar y adoptar medidas que, aunque supongan una injerencia en los derechos civiles de los ciudadanos, sean también necesarias, proporcionadas y respetuosas con la esencia de los derechos afectados, pero que, al mismo tiempo, ofrezcan herramientas a los investigadores y autoridades judiciales para que, como mínimo, se equilibre la capacidad de actuación entre quienes legítimamente velan por la seguridad de los ciudadanos y quienes abusan de los legítimos avances tecnológicos, tanto de los actuales como de los disponibles en un futuro próximo (cifrado de datos de forma generalizada, 5G, IA, Internet de las Cosas, etcétera). Creemos que [por suerte], ante una incorrecta actuación de las agencias encargadas de la aplicación de la ley, existen

controles adecuados y precisos para detectar esas conductas y corregirlas y que no se justifica la sospecha de *tecnovigilancia* que en ocasiones se quiere proyectar. En ese sentido, nos parece interesante la idea propuesta por Rodotà (que citamos en la pina 38) respecto de la posibilidad de establecer un *habeas data* similar al *habeas corpus*, pero en el mundo lógico, aunque quizás solo sea poner un nombre diferente a una institución jurídica ya existente y que se puede extender igualmente a las actuaciones que aquí venimos analizando.

Novena. El impulso principal para llegar a una solución sobre qué camino seguir para encontrar la *clave de bóveda* que permita reconducir la situación generada tras la invalidación de la Directiva no depende tanto de los afectados directamente por la aplicación de la norma europea (ciudadanos, sector profesional de las telecomunicaciones o policías y jueces), sino de los decisores políticos europeos y de los Estados miembros, que deben reunirse en Bruselas con una visión amplia y de conjunto y con una apuesta europea que supere las visiones puramente nacionales -todos cedemos para ganar todos- y que deben hacer una propuesta lo antes posible sobre la que modular las posiciones y consensuar las medidas a adoptar. Nos puede parecer una idea básica que no habría que reflejar en un estudio de estas características, pero la experiencia en el proceso legislativo europeo nos lleva a concluir que son muy frecuentes las negociaciones en las que se vislumbra claramente que la falta de acuerdo está precisamente en que se pretende imponer la solución nacional propia como la más idónea para el resto de los miembros de la Unión, y -lógicamente- no suele ser aceptado por el resto. En consecuencia, se malogran las propuestas iniciales [trabajadas de forma unitaria y con una idea clara sobre los objetivos a cumplir y la forma de alcanzarlos] o se alargan los expedientes hasta el punto de que se suele perder la perspectiva inicial y, en ocasiones, al final se causa más perjuicio que si no se hubiera intentado cambiar la situación anterior a la propuesta.

En la negociación de la Directiva de conservación de datos, hubo desde el principio numerosas críticas que partían de diferentes ámbitos (de instituciones y agencias europeas, el SEPD o el GT del Artículo 29), que no fueron tenidas en cuenta, pero que avisaban de la desproporcionada injerencia en los derechos fundamentales de

los ciudadanos. Después se confirmó que tenían un criterio acertado. Dentro de la dinámica propia del procedimiento europeo de producción normativa, se observa también que frecuentemente se obviaban los informes, no vinculantes, de determinados organismos; especialmente si suponían un freno considerable al avance de la propuesta, debido muchas veces a la urgencia en la adopción de las medidas (por motivos que apuntábamos antes). Por suerte, esta dinámica está cambiando, en la idea de que la aportación de todos contribuye al enriquecimiento del texto y, sobre todo, evita recursos a los tribunales y eventuales situaciones de invalidación. En ese sentido, la Directiva PNR, sobre la que hemos comparado determinados aspectos de la Directiva 2006/24/CE, ha tenido un recorrido parecido en cuanto a que surgió como medida urgente, se basa en obligaciones impuestas a operadores privados para la conservación y transferencia de datos a las agencias encargadas de la aplicación de la ley, se sustenta sobre fines parecidos y con medidas de conservación y acceso a los datos también con ciertas similitudes y, sin embargo, no ha sido tan cuestionada antes ni durante el procedimiento legislativo, ni instada la actuación del Tribunal europeo (salvo un caso concreto que dio lugar al Dictamen 1/15).

Décima. Aun siendo fundamental contar con debates a nivel de expertos respecto de las ideas/opciones antes apuntadas, es importante también a nivel político adoptar una orientación sobre el mejor enfoque para los próximos pasos a seguir, que sirva de guía, apoyo e impulso a los técnicos.

Lo que no es discutible es la necesidad de consenso a nivel político entre los dirigentes europeos, a nivel de ministros de justicia e interior, por ser los primeros receptores del contenido de las discusiones que se desarrollan en el seno del Consejo de la UE; y, en segundo lugar, en un escalón superior, de los jefes de Estado y de gobierno, en las reuniones periódicas del Consejo Europeo. Solo de esta forma, y a través de la búsqueda de puntos de encuentro con el Parlamento Europeo, se podrá alcanzar una solución a un problema que se presentó como urgente en 2017 [y lo era], pero sobre el que no se ha sabido identificar una línea clara de trabajo hacia una solución que satisfaga a todos los implicados/afectados. Mientras tanto, cada vez tienen menos argumentos los tribunales nacionales para seguir aplicando la normativa que se adoptó

tras la aprobación de la Directiva de 2006. El coste en tiempo, recursos y generación de frustración que puede acarrear el que sean archivadas o declaradas nulas investigaciones que llevan años en curso, basadas muchas de ellas en gran medida en datos que se obtuvieron y trataron en virtud de la normativa de conservación de datos, exige avanzar con rapidez en los foros europeos.

Undécima. Mientras algunos Estados miembros, o bien han modificado su legislación nacional para adaptarla a la jurisprudencia reciente o simplemente han dejado de aplicarla, la mayoría las siguen considerando ajustadas a Derecho. Lo cierto es que, a la vista de las últimas sentencias del TJUE, mantener la validez de las normativas nacionales resulta prácticamente imposible. Así las cosas, cabe concluir que la aplicabilidad de la norma nacional en materia de conservación de datos *ha muerto,* si no lo había hecho ya antes. Esto, lógicamente, tiene consecuencias urgentes e importantes sobre casos actuales o en revisión, pero también futuros. En consecuencia, creemos que no caben ya más excusas para enfocar el problema desde el convencimiento de la necesidad de un cambio profundo.

Indudablemente, el Tribunal de Luxemburgo, al menos en este caso concreto, ha ido avanzando hacia la determinación de criterios específicos sobre cómo respetar los derechos fundamentales que recoge la Carta, en materias puramente de justicia penal, incluso descendiendo a la casuística concreta. Creemos que, a pesar de la tradicional reticencia de los Estados miembros a *comunitarizar* políticas en este ámbito por la evidente cesión de soberanía en favor de la Unión Europea, el incremento en el recurso al Tribunal europeo por parte de los nacionales hace que se vaya delimitando el marco sobre el que esas políticas tendrán que descansar. Todavía no es pacífico el debate acerca de si los asuntos de justicia e interior deben o no ser abordados a nivel de la Unión. Sin embargo, no cabe duda de que, contando con reglas claras y precisas, se podrá ganar en eficacia y eficiencia en la adopción de las medidas.

Decimosegunda. El principio de proporcionalidad se ha previsto para resolver conflictos entre derechos, sin establecer jerarquías apriorísticas. La Directiva impuso

obligaciones a los proveedores de servicios respecto de las que no se discutió que respondieran al interés general, pero si su necesidad y proporcionalidad, en la medida en que no se valoró si las medidas adoptadas producían una invasión menor que otras a la hora de alcanzar el mismo objetivo, como tampoco incorporaban normas claras que indicaran a los ciudadanos en qué circunstancias se podían conservar sus datos. En consecuencia, creemos fundamental que, de forma general, para los distintos casos presentes y futuros de elaboración de normas europeas [serviría el mismo criterio para la producción normativa nacional] se siga una guía como la que ha presentado el Supervisor Europeo de Protección de Datos, como orientación técnica respecto de las pruebas de necesidad y proporcionalidad que se han de realizar ante cualquier propuesta. Una vez más, apostamos por un enfoque integral desde el origen, que evite pérdida de tiempo y efectos indeseables tanto para la libertad de actuación y expresión de los ciudadanos como para la actuación de los servicios policiales y otras agencias encargadas de la aplicación de la ley.

No hemos analizado cómo operaría el consentimiento del suscriptor de un servicio de telecomunicaciones -o de quien se descarga una aplicación u otro servicio digital en su Smartphone- respecto de la conservación de los datos que se generan por medio de sus comunicaciones electrónicas, de acuerdo con lo previsto en la normativa europea en la materia (fundamentalmente el Reglamento General de Protección de Datos de 2018). No obstante, creemos que sería muy pertinente realizar un estudio sobre su viabilidad y las ventajas e inconvenientes de tal medida. Por supuesto, el consentimiento sería voluntario. Somos conscientes de que se perdiera gran parte de los datos, especialmente los de aquellos que están dispuestos a delinquir, que no lo otorgarían, pero estamos convencidos de que una parte importante de la sociedad lo vería necesario y proporcionado, especialmente si se explica con rigor y minuciosidad el objetivo que persigue contar con la colaboración ciudadana a este respecto.

Decimotercera. El TJUE invalidó la Directiva en 2014, por considerar que autorizaba una injerencia especialmente grave en determinados derechos fundamentales recogidos en la Carta (privacidad, protección de los datos de carácter personal y, con dudas, también libertad de expresión), sin garantizar adecuadamente los principios de

necesidad y proporcionalidad. Desde entonces, tras las sucesivas sentencias que han seguido a la del *Caso Digital Rights Ireland*, no ha variado su posición inicial, consolidando así una doctrina que, además, ha sentado determinados principios que no solo tendrán implicaciones en el sistema de conservación de datos de comunicaciones electrónicas que se pueda aprobar en la Unión, sino también en otros ámbitos relacionados con el tratamiento de datos para fines de prevención y lucha contra la delincuencia grave y otras amenazas a la seguridad pública. En ese sentido, el Tribunal dictamina que ni siquiera las obligaciones de los Estados miembros respecto de la garantía de la seguridad de los ciudadanos puede tener por efecto la justificación de injerencias tan graves como las que se producían a través de las medidas que establecía la Directiva, a través de la conservación de los datos de tráfico y de localización de prácticamente toda la población, sin que esos datos de las personas afectadas guarden una relación, al menos indirecta con el objetivo perseguido. Entendemos que, de esa forma, establece una gradación respecto de la importancia de unos derechos y otros de los recogidos en la CDFUE, decantándose por la privacidad y la protección de los datos de carácter personal.

Decimocuarta. Actualmente, la única posibilidad que existe para aprobar una nueva norma europea de conservación de datos de las comunicaciones electrónicas es a través de la excepción que recoge el artículo 15, apartado 1 de la Directiva 2002/58/CE, para los supuestos que en este artículo se recogen. Sin embargo, desde hace ya varios años se está elaborando un nuevo reglamento que sustituya a la Directiva de 2002. El trabajo desarrollado hasta ahora prevé que el borrador consensuado a nivel del Consejo de la Unión Europea incorpore nuevos artículos (que hemos tratado) que prevén mantener la cláusula habilitante para el nuevo marco de conservación, incorporando además ciertos matices que aclaran más la situación. Sin embargo, se desconocen las negociaciones en curso con el otro colegislador (Parlamento Europeo) y si finalmente se acordará una redacción igual o similar o si se limitará más aún el margen de maniobra. En el segundo caso, se dificultaría mucho más un acuerdo posterior para el nuevo régimen de conservación por el que abogamos y, de ser así, presumimos que se recurriría a soluciones nacionales que no resolverán la situación. Una vez más, el trabajo conjunto y coordinado entre los expertos, en este caso de los ámbitos de telecomunicaciones y de justicia e interior, es clave. Y la búsqueda del mayor consenso

posible entre los Estados miembros para otorgar a la presidencia de turno de la Unión Europea ideas claras y líneas rojas sobre las que basar su negociación es obligatoria, para mantener la redacción del borrador de reglamento como consta en la orientación general que aprobó el Consejo de la UE a comienzos de 2021, de cara a una solución europea a la conservación de datos de las comunicaciones electrónicas.

Decimoquinta. El Tribunal ha recordado a los investigadores lo que ya conocen perfectamente, al indicar que la eficacia de una investigación no depende de un solo medio (o conjunto de medios). Cuando se defiende de la forma que se está haciendo en este caso la posibilidad de conservar los datos a los efectos de la investigación penal, no es a cambio de la renuncia al uso de otros medios de investigación que permitan también establecer vínculos entre sospechosos o la búsqueda de víctimas de delitos, o la confirmación de la no participación de una determinada persona; sino porque en muchas ocasiones es el elemento principal sobre el que basar las evidencias o pruebas de la comisión de un delito grave. Ante determinados ilícitos penales, principalmente cometidos a través de Internet, es la única vía para comenzar una investigación que posteriormente se irá complementando con otras acciones. Por tanto, interpretamos esa afirmación del Tribunal europeo como una vía para llamar la atención a los tribunales nacionales ante la reiterada solicitud de parecer sobre cuestiones que considera ya resueltas.

Decimosexta. El Tribunal ha diferenciado entre finalidades de la conservación de datos (seguridad nacional, prevención y lucha contra la delincuencia grave; u otras investigaciones sobre delitos no graves) así como entre categorías de datos (de tráfico y de localización, de identidad civil de usuarios y suscriptores; y de las IP de origen de una comunicación), permitiendo una mayor o menor injerencia en los derechos afectados, como hemos analizado en el capítulo VI. Aunque nos parece que la delimitación que hace ayudará a concretar el próximo régimen de conservación de datos, creemos también -y así lo indicábamos antes- que está adoptando en cierto modo el rol de legislador, por cuanto cita expresamente las distintas tipologías de conservación que se pueden aceptar e incluso los criterios para señalar unas y otras.

Por otro lado, relacionado con lo anterior, en la medida en que desciende en las sentencias casi al detalle de cómo se reflejaría cada uno de los supuestos en la norma (directiva o reglamento) que pudiera aprobarse, hemos de señalar que en los pocos matices que se ofrecen desde la posición inicial hasta la última sentencia (de octubre de 2022), se observan también ciertas incoherencias argumentativas, como el hecho de que uno de los supuestos que le llevaron a considerar la gravedad de la injerencia en los derechos era el periodo de conservación de datos; sin embargo, cuando la ley alemana se modifica y, buscando subsanar esta deficiencia, introduce periodos de conservación extremadamente cortos (a nuestro entender, claramente insuficientes para cualquier tipo de investigación compleja o conocida pasado un tiempo desde la comisión del hecho delictivo), el Tribunal se pronuncia indicando que el periodo de conservación no es relevante a los efectos de la injerencia, ya que esta produce desde el mismo momento en que se conservan los datos.

Decimoséptima. Uno de los supuestos respecto de los que se pueden establecer medidas como excepción al artículo 15, apartado 1 de la Directiva de privacidad de las comunicaciones electrónicas es la prevención de las amenazas a la seguridad nacional. De hecho, este es el único caso en el que permite, siempre bajo estrictas salvaguardias, una conservación generalizada e indiscriminada. De las amenazas más previsibles y probables que puedan provocar un riesgo cierto y grave a las estructuras del Estado o a la población general, está el terrorismo; de hecho, la amenaza terrorista mundial, y en Europa en particular (con acciones concretas y en pocos años en diversos Estados miembros), es la que concitó el consenso entre los responsables políticos de los Estados miembros y el acuerdo en las instituciones europeas acerca de la necesidad de adoptar medidas concretas; entre ellas, la aprobación de la Directiva de 2006. No obstante, la materialización de ese propósito es lo que no obtuvo el mismo nivel de consenso. Aun así, permanece la necesidad.

La disparidad de supuestos permitidos y prohibidos respecto de la finalidad de protección de la seguridad nacional y de la lucha contra la delincuencia grave, nos lleva a considerar como más idóneo que se traten de forma separada. Por ello, en el capítulo IX hemos presentado las propuestas que, a nuestro entender, podrán delimitar el marco

del nuevo sistema de conservación únicamente para la prevención, investigación, persecución y enjuiciamiento de delitos graves; no así las correspondientes a la seguridad nacional, porque, aunque estén también sometidas al respeto de los derechos fundamentales que proclama la Carta, deja más margen de actuación a los Estados miembros, y mezclar ambas finalidades de conservación podría generar problemas de interpretación sobre cuándo se está en unos u otros casos y qué medidas se pueden adoptar en cada uno de ellos. De hecho, algunos Estados miembros han planteado ante el TJUE la legalidad de acceder a los datos conservados con fines de prevención de la seguridad nacional también cuando se presenta una necesidad para la investigación de un hecho concreto de delincuencia grave. En otras propuestas legislativas de la Unión Europea también se usa la técnica de aprobar un *paquete de medidas* a través de un reglamento y una directiva o más de un reglamento. Este podría ser un caso para ello, que la Comisión Europea debería analizar.

Sobre lo que no parece tener dudas el Tribunal europeo, y estamos de acuerdo con ello, es que no se puede acceder a los datos conservados con ocasión de una amenaza grave a la seguridad nacional, para ser explotados en el ámbito de la delincuencia grave. Permitir esa acción sería establecer lo que en otros ámbitos se conoce como *puerta trasera*, y no es admisible. Hemos de reconocer que, en algún momento de la negociación del borrador de reglamento de privacidad de las comunicaciones electrónicas, se ha planteado por algún Estado miembro la posibilidad de excluir del ámbito de aplicación de la norma las cuestiones relacionadas con la seguridad nacional, e incluso las correspondientes a la seguridad pública y la investigación penal, no con carácter excepcional, como ocurre ahora, sino en toda su extensión, basándose en argumentos -entre otros- como que en esas situaciones prevalecen las constituciones nacionales. Hoy no obtendría apoyo ni siquiera en el ámbito de las discusiones del Consejo, es decir, no habría consenso por parte de la mayoría de los países, máxime cuando el Alto Tribunal se ha pronunciado claramente al respecto en su análisis del alcance del artículo 15, apartado 1 de la vigente Directiva sobre privacidad de las comunicaciones electrónicas de 2002.

En cambio, la norma sí debe recoger el resto de los supuestos, las tipologías de datos y los criterios de conservación para cada uno de ellos, además de las medidas de seguridad física y lógica para su custodia, tratamiento por los proveedores, técnicas de enmascaramiento y borrado posterior, etcétera, según hemos explicado con detalle en el capítulo anterior (correspondiente a las propuestas que han resultado tras nuestra investigación).

Decimoctava. Respecto del acceso a los datos, a pesar de que el Tribunal no se había pronunciado en las primeras sentencias, sí lo ha hecho en las últimas, determinando que no se puede salvar la conservación injustificada mediante garantías reforzadas para el acceso. Por tanto, se obliga a las autoridades judiciales y administrativas habilitadas a valorar si la conservación es necesaria y proporcionada, antes de autorizar o no el acceso y tratamiento. Aun así, las decisiones y las acciones quedan sometidas al criterio de las autoridades nacionales, por lo que creemos conveniente que no se regule a través de la norma europea, salvo meras referencias al criterio antes reseñado, para no constreñir a los jueces nacionales en su libertad de valoración de la prueba, que en cierto modo ha quedado *cuestionada o matizada* por el TJUE.

Decimonovena. La inexistencia de una definición precisa y consensuada a nivel europeo respecto del concepto de delito grave dificulta la adopción de medidas homogéneas y un tratamiento armonizado de la información conservada en cada uno de los países y en su intercambio con el resto a través de los mecanismos establecidos para ese propósito. Sin embargo, este no ha sido un obstáculo para aprobar otras normas, como la Directiva PNR, que también basan sus acciones en gran medida en la prevención de la comisión de delitos graves. Para ello, en el caso de la PNR se ha recurrido a una lista cerrada, incluida en un anexo, con aquellos delitos que se han considerado como graves (en base fundamentalmente a una determinada pena de prisión). Aun así, la labor de la autoridad judicial o administrativa independiente será crucial y garante de que las medidas se adaptan a la gravedad del delito de cada caso.

Vigésima. El propio Tribunal apela a agudizar el ingenio en la búsqueda de otros criterios a los indicados en sus sentencias para establecer un mecanismo de conservación selectiva. No obstante, como decíamos anteriormente, una investigación suele basarse en diferentes medios de obtención de pruebas. E incluso en el ámbito de los datos generados por los ciudadanos en sus comunicaciones electrónicas, hay muchos datos que no están sometidos al ámbito de aplicación de la normativa sobre privacidad electrónica y, en consecuencia, sobre los que se puede obtener también una valiosa información a la hora de investigar delitos graves. A modo de ejemplo, siguiendo la dinámica casuística del TJUE, citaremos algunos de ellos, que no se generan como consecuencia de una comunicación entre dos usuarios, sino que se almacenan en un dispositivo concreto: el historial de ubicaciones mediante la consulta de determinadas aplicaciones o pinas web (el tiempo, mapas, aplicaciones de deporte y toda la variedad de información que recoge, datos de salud, etcétera); o la localización del GPS de los vehículos, o patinetes y bicicletas eléctricas, etcétera.

Muchas de estas aplicaciones se incardinan dentro de la denominación de OTT, no recogidas actualmente en las obligaciones de la vigente Directiva de privacidad de las comunicaciones electrónicas, pero sí en el borrador de reglamento que la modificará. Antes nos referíamos a aquellos datos que se almacenan en el terminal pero que no se han generado en una comunicación con otra persona o usuario; pero algunas de estas permiten también compartir esa información con otras personas a través, a su vez, de otras aplicaciones. En definitiva, teniendo en cuenta que la mayoría de las comunicaciones se producen actualmente mediante OTT y que la tendencia es a aumentar, es obligatorio que se incluyan en la nueva norma sobre privacidad electrónica y que el nuevo marco de conservación de datos pueda servirse también de los datos conservados por los proveedores de estos servicios, que actualmente aplican normas de conservación para fines de negocio y comercial muy dispares.

Vigésima primera. Es indudable que el nuevo régimen de conservación supondrá un cambio de paradigma con implicaciones también en términos de incremento de los recursos necesarios para el desarrollo de las investigaciones, pero sobre todo para la autoridad judicial o administrativa que tenga que analizar las

solicitudes y realizar la prueba de necesidad y proporcionalidad previo a la autorización o denegación, así como la revisión posterior del cumplimiento de los requisitos para su mantenimiento o decaimiento de las medidas adoptadas, etcétera. En consecuencia, a la clásica lentitud en la toma de decisiones en los procesos de investigación penal habrá que añadir más dilación. Supondrá también costes incrementados para los proveedores de servicios, por las medidas adicionales que tendrán que sufragar para garantizar la seguridad de los datos almacenados y su transferencia, aunque puede que no sean excesivamente gravosos, teniendo en cuenta que ya deben adoptar esas medidas para aquellos datos que conservan con fines de negocio y facturación.

Respecto de la autorización, las diferencias entre los sistemas judiciales y las normas procesales entre los Estados miembros se manifiestan también en el hecho de que pueda ser una autoridad administrativa quien realice esa labor de autorización, mientras que se excluye al ministerio fiscal, por considerar que no reúne el requisito de independencia respecto de las investigaciones; lo que no deja de ser pintoresco, al menos desde la realidad procesal de nuestro país. En España no se generan estos problemas.

Vigésima segunda. Por último, es indudable que los avances tecnológicos continúan produciéndose a una velocidad cada vez mayor (ya se está trabajando contrarreloj por implementar las tecnologías 5G que permitan cumplir con las expectativas que despierta el Internet de las Cosas- IoT) y deben aprovecharse para proporcionar una vida mejor a los ciudadanos europeos, a los que, al mismo tiempo, debe proporcionarse un acceso general y seguro a Internet, garantizando que este sea también respetuoso con los derechos fundamentales de los ciudadanos. Pero al mismo tiempo es una obligación también de nuestros gobernantes garantizar que esa seguridad lo sea también respecto de aquellos que aprovechan la tecnología y el anonimato que esta ofrece, para cometer delitos y conculcar otros derechos igualmente importantes y sobre los que las autoridades, en concreto las policiales y judiciales, tienen un deber constitucional. El nuevo marco europeo de conservación de datos a los efectos de prevenir, investigar, perseguir y enjuiciar delitos graves debe ser ambicioso e intentar dejar la puerta abierta *–no una puerta trasera-* para poder adaptarse a esos nuevos

desarrollos tecnológicos y, para ello, es imprescindible participar con los fabricantes y desarrolladores europeos e internacionales desde la concepción de la tecnología para que tengan en cuenta los intereses legítimos en la lucha contra la delincuencia grave. No se entendería que, después de casi dos lustros y tanto esfuerzo, se aprobara una norma que quedara obsoleta nada más echar a andar.

BIBLIOGRAFÍA, DOCUMENTOS Y JURISPRUDENCIA

AGUILERA MORALES, M., *"El exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas"*, Boletín del ministerio de justicia estudio doctrinal, nº 2145, Año LXVI, agosto de 2012, pp. 1- 29, en https://dialnet.unirioja.es/descarga/articulo/3986762.pdf

ALONSO GARCÍA, R., *"Lisboa y el Tribunal de Justicia de la Unión Europea"*, Papeles de Derecho Europeo e Integración Regional, Instituto de Derecho Europeo e Integración Regional (IDEIR), Universidad Complutense, núm. 1, 2013, pp. 1-30

ARANDA ÁLVAREZ, E., *"La alerta temprana en el procedimiento legislativo de la Unión Europea. Una reflexión sobre su utilidad desde la reciente experiencia española"*, Revista de Derecho Comunitario Europeo, nº. 44, 2013, pp. 101-153.

ARROYO ROMERO, F.J., *La influencia de Europol en la comunitarización de la policía europea*, Ediciones Akal, Madrid, 2006.

BAGGER TRANBERG, C., *"Proporcionalidad y protección de datos en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas"*, International Data Privacy Law, 2011, Vol. 1, nº 4, pp. 239-248.

BAHAMONDE BLANCO, M., "Medidas de investigación tecnológica a la luz de los Derechos Fundamentales, una cuestión pendiente", Diario La Ley, núm. 9160, 2018, en http://data.europa.eu/eli/reg/2016/794/oj

BALLASCHK, J., *"In the unseen realm: transnational intelligence sharing in the European Union- Challenges to fundamental rights and democratic legitimacy"*, Standford Journal of International Law, 51, 2015, pp. 19-51.

BALLESTEROS MOFFA, L.A., *"La revisión del régimen jurídico de la privacidad en la Unión Europea"*, Revista del posgrado en derecho de la UNAM, Nueva época, núm. 8, 2018, pp. 38-68.

BRANDARIZ GARCÍA, J.A. *"¿Una teleología de la seguridad sin libertad? La difusión de lógicas actuariales y gerenciales en las políticas punitivas"*, en Fundamentos nº 8, La Metamorfosis del Estado y del Derecho, Universidad de Oviedo, 2014, pp. 313-354, https://www.unioviedo.es/constitucional/fundamentos/octavo/pdfs/Brandariz-Teleologia.pdf

BYGRAVE, L.A., *"Data Privacy Law. An International Perspective"*, Oxford University Press, 2014.

CAPATORTI, F., *"El procedimiento de producción legislativa en las Comunidades Europeas"*, 1986, en Revista Española de Derecho Constitucional, pp. 127-154.

CASTELLANOS CLARAMUNT, J., *"Transparencia y participación ciudadana: la lucha contra la corrupción como eje vertebrador del proceso democrático"*, Revista Española de la Transparencia, nº 15, 2022, pp. 107-129.

COLOMER HERNÁNDEZ, I., *"La cesión de datos de las comunicaciones electrónicas para su uso en investigaciones criminales: una problemática en ciernes"*, en Jiménez Conde, F.J (dir.), *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales*. Valencia, Tirant lo Blanch, 2018, pp. 77-100.

CONDE ORTÍZ, C., *La protección de datos personales un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid, Dykinson, 2005

CUBERO MARCOS, J.I., y ABERSTURI GORRIÑO, U., "*Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007, sobre conservación de datos"*, Revista Española de Derecho Constitucional, núm. 83, 2008, pp. 175-197.

DE WITTE, B., *"The past and the future role of the European Court of Justice in the Protection of Human Rights"*, ALSTON, P., (Ed) The EU and the Human Rights, OUP, 1999.

DÍEZ-HOCHLEITNER, J., *"El derecho a la última palabra: ¿Tribunales constitucionales o Tribunal de Justicia de la Unión"*, Papeles de Derecho Europeo e Integración Regional, nº17, 2013, pp. 1-38.

ETXEBERRIA GURIDI, J.F., *"Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo"*, Eguzkilore, nº. 23, San Sebastián, 2009, pp. 351-366

FERNÁNDEZ BARBUDO, C., *"Hacia una privacidad colectiva: repensar las bases teóricas de la distinción público/privado en la economía de la vigilancia"*, Teknokultura, Revista de Cultura Digital y Movimientos Sociales, Ediciones Complutense, 2019, pp. 69-76.

FERNANDEZ-LASQUETTY, J. y BELLO, M., *"La legislación europea no permite una normativa nacional que recopile datos de tráfico y localización de manera indiscriminada. Sentencia del Tribunal de Justicia de 21 de diciembre de 2016, Tele2 Sverige (C-203/15 y C-698/15)"*, en Anuario Elzaburu de jurisprudencia europea en propiedad industrial e intelectual, en http://www.elzaburu.es/en/document-centre/search-news-items?op=viewcms&id2=3005116

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

FERNÁNDEZ RODRÍGUEZ, J.L., *"Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente, en Centro de Estudios Políticos y Constitucionales*", Revista Española de Derecho Constitucional, nº. 108 (septiembre/diciembre 2016), pp. 93-122.

FIGUEROA NAVARRO, M.C., *"El conflicto intimidad/información: un análisis jurisprudencial"*, en Anuario de derecho penal y ciencias penales, Tomo 49, Fasc/Mes 3, 1996, pp. 943-978

GARCÍA SANZ, R.M., *"Redes sociales online: fuentes de acceso público o ficheros de datos personales privados (Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas)"*, 2011, Revista de derecho político, UNED, nº 81, 2011, pp. 101-154

GARCÍA-VADECASAS Y FERNÁNDEZ, R. y CARPI BADÍA, J.M., *"El Tribunal de Justicia de la Unión Europea. Algunas consideraciones respecto a su papel en el marco de la construcción europea"*, en Revista Jurídica de CyL, nº. 3, 2004, pp. 13-48.

GARZÓN CLARIANA, G., *"El Parlamento Europeo y la evolución del poder legislativo y del sistema normativo de la Unión Europea"*, Revista de Derecho Comunitario Europeo, nº. 50, 2015, pp. 43-83

GERALDES DA CUNHA LOPES, T.M., *"El derecho a la intimidad y la protección de datos en la era de la Seguridad global. Principios constitucionales versus riesgos tecnológicos"*, Anuario Jurídico y Económico Escurialense, núm. 48, 2015

GONZÁLEZ DE LA GARZA, L.M., *Comunicación Pública en Internet*, Creaciones Copyright, Madrid, 2004

GONZÁLEZ PASCUAL, M.I., *"El Tribunal Constitucional federal alemán ante la compatibilidad con los derechos fundamentales de la normativa nacional de origen europeo de prevención de delitos"*, Revista de Derecho Comunitario Europeo, núm. 34, 2009, pp. 945-966.

- *"El TJUE como garante de los derechos en la UE a la luz de la Sentencia Digital Rights Ireland"*, en Revista de Derecho Comunitario Europeo, nº. 49, Madrid, septiembre/diciembre 2014, pp. 943-971.

- *"Criminal Law as an Essential Function of the State: Last Line of Resistance?"* en SAIZ ARNAIZ, A., ALCOBERRO LLIVINA, C. (eds.) National Constitutional Identity and European Integration, Intersentia, Antwerp, 2013, pp. 159-175.

HUSTINX, P., "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, pp. 1-52, p. 15, en: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

KLIP, A., *"European Criminal Law, An Integrative Approach"*, 4th *Edition, Intersentia, 2021, pp. 121-130.*

LENAERTS, K., VAN NUFFEL, P., *European Union Law, Sweet and Maxwell*, 3ª edition, Londres, 2011

LÓPEZ AGUILAR, J.F., *"La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU"*, UNED, Teoría y Realidad Constitucional, núm. 39, 2017, pp. 557-581.

LÓPEZ BARAJAS, I., *"El deber de conservación de datos en la Unión Europea y sus límites"*, en Revista de Derecho de la Unión Europea, nº 16, 2009, pp. 195-220.

LÓPEZ ESCUDERO, M., *"Primacía del Derecho de la Unión Europea y sus límites en la jurisprudencia reciente del TJUE",* Revista de Derecho Comunitario Europeo, 64, 2019, pp. 787-825.

MANGAS MARTÍN , A. y LIÑAN NOGUERAS, D.J, *Instituciones y Derecho de la UE, Tecnos*, 10ª Edición, 2020

- *"La reforma institucional en el Tratado de Reforma"*, en Revista de las Cortes Generales, 2007, pp. 127-154.

MARSAL MUNTALÁ, J., *"Seguridad versus Libertad"*, 2005, pp. 219-226, en http://arbor.revistas.csic.es

MARTÍNEZ DE PISÓN, J., *"El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional"*, Anuario de Filosofía del Derecho, núm. 32, 2016, pp. 409-430.

MARTÍNEZ, R., *"Safe Harbor: retos para el modelo europeo de la privacidad"*, en Lefebvre – El Derecho, 19.10.2015, en http://tecnologia.elderecho.com/tecnologia/privacidad/SafeHorbor-modelo-europeo-privacidad_11_874180003.html

McINTYRE, T.J., *"Data retention in Ireland: Privacy, policy and proportionality"*, Computer Law and Security Review, Vol. 24, Issue 4, 2008, pp. 326-334, https://ssrn.com/abstract=2426208

MINERO ALEJANDRE, G., *"Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea"*, Anuario Jurídico y Económico Escurialense, 2017, pp. 13-58

MITSILEGAS, V., GUILD, E, KUSKONMAZ, E. Y VAVOULA, N., *"Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks". Eur Law J. 2022*, pp. 1-36

MORENO CATENA, V., *"El cambio de paradigma y el principio de reconocimiento mutuo y sus implicaciones. Perspectivas del Tratado de Lisboa"*, en Escuela Judicial, Consejo General del Poder Judicial, 2013, pp. 1-57.

NIEVES SALDAÑA, M., *"The right to privacy: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de*

Warren y Brandeis", UNED, Revista de Derecho Político, núm. 85, 2012, pp. 195-240.

ORDOÑEZ SOLIS, D., *La protección judicial de los derechos en internet en la jurisprudencia europea, Reus*, Madrid, 2014

OROMÍ I VALL-LLOVERA, S., *"Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE"*, Revista de Internet, Derecho y Política, núm. 31, pp. 1-13.

ORTÍ VALLEJO, A. *Derecho a la intimidad e informática, Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada, Comares*, Granada, 1994

ORTIZ PRADILLO, J.C. *"Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas"*, Revista General de Derecho Procesal, núm. 52, 2020, pp. 1-28.

- *"Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de datos de tráfico de las comunicaciones electrónicas"*, La Ley Penal, nº 75, octubre, 2010

- *"El impacto de la tecnología en la investigación penal y en los derechos fundamentales"*, en Problemas actuales de la justicia penal, Madrid, 2013, pp. 317-341

PERALTA GUTIÉRREZ, A., y AGUIRRE ALLENDE, P., *"El TJUE y el acceso a los datos de abonado en el seno de la instrucción penal"*, en Diario La Ley, nº. 9420, Sección Tribuna, 22 de mayo de 2019, Wolters Klumer, pp. 1-17

PERALTA GUTIÉRREZ, A, "*La necesaria regulación de la vigilancia masiva: Casos Quadrature du Net y Big Brother Watch"*, Diario La Ley, nº. 9973, 2021, en , en https://diariolaley.laleynext.es/dll/2021/12/17/la-necesaria-regulacion-de-la-vigilancia-masiva-casos-quadrature-du-net-y-big-brother-watch

PÉREZ ESTRADA, M.J., *"La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información"*, Universidad del País Vasco, 2019, pp. 1297-1330.

PÉREZ LUÑO, A.E, *"Las generaciones de derechos humanos"*, Universidad de Sevilla, Revista del Centro de Estudios Constitucionales, núm. 10, 1991, pp. 203-217.

- *"Del habeas corpus al habeas data"*. Conferencia impartida el 11 de mayo de 1990, XIV Curso de Informática y Derecho, Centro Regional de la UNED de Extremadura. Curso sobre Informática y Derecho, 1990, pp. 153-161 en https://dialnet.unirioja.es/descarga/articulo/4482974.pdf

PÉREZ ROYO, J., *"La democracia frente al terrorismo global, Terrorismo, democracia y seguridad"*, en Perspectiva constitucional, Barcelona, 2010, pp. 7-12.

PERRY, A., RUBINSTEN, O., PELED, L. y SHAMAY-TSOORY, S. *"Don't stand so close to me: A behavioral and ERP study of preferred interpersonal distance"*, Neuroimage, 83, 2013, pp. 761-769.

PESQUEIRA ZAMORA, M.J., *"Diligencias de investigación, cesión de datos y principio de proporcionalidad"*, Universidad Abat Oliba, InDret, 2020, pp. 419-445

PIÑAR MAÑAS, J.L. *"El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas"*, Cuadernos de Derecho Público, 19, 2003, pp. 45-90.

POLO ROCA, A., *"Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos"*, Universidad de Deusto, vol. 69/1, enero-junio 2021, pp. 211-240

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

- *La conservación de datos en el sector de las telecomunicaciones: un estudio sobre su regulación en la Unión Europea y su cabida en el Derecho de la Unión, Thomson Reuters, Aranzadi*, Pamplona, 2022

PUERTO, M.I y SFERRAZZA TAIBI, P., *"La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional"*, en Revista Derecho del Estado, núm. 40, enero-junio de 2018, pp. 209-236

RALLO LOMBARTE, A., *"El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet*", UNED, Teoría y Realidad Constitucional, núm. 39, 2017, pp. 583-610.

REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea, Dykinson,* Madrid, 2008.

RENDA, A., *"Policymaking in the EU: achievements, challenges and proposals for reform". Brussels: Centre for European Policy Studies (CEPS), 2009, pp. 1-90.*

RIDAURA MARTÍNEZ M.J.: *"La seguridad ciudadana como función del Estado"*, Estudios de Deusto, 2014, pp. 319-346.

RIZZO, G., *Derecho a la privacidad y seguridad en el espacio público europeo*, tesis doctoral, Universidad Carlos III de Madrid, 2019

ROCA TRIAS, E., *"Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española"*, XV Conferencia Trilateral, 24-27 de octubre de 2013, Roma

RODOTÀ, S., *"La conservación de los datos de tráfico en las comunicaciones electrónicas"*, en Segundo Congreso sobre Internet, derecho y política: análisis y prospectiva, http://www.uoc.edu/idp/3/dt/esp/rodota.pdf, pp. 53-60.

RODRÍGUEZ GARCÍA, L.F., *La Directiva europea sobre Conservación de Datos de las Comunicaciones Electrónicas y su transposición en el Derecho español*, tesis doctoral UNED, Madrid, 2013, en http://e-spacio.uned.es/fez/view/tesisuned:Derecho-Lfrodriguez

RODRÍGUEZ LAINZ, J.L., *"El renacer de la Ley Española sobre conservación de datos relativos a las comunicaciones (Comentario a la STJUE, Gran Sala, de 6 de octubre de 2020)"*. Diario La Ley, 2020, nº. 9740

- *"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 Commissioner an Garda Síochána"*, Diario La Ley, nº. 10058, Sección Tribuna, 2022, en https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1CTEAAmNTI2MDI7Wy1KLizPw8WyMDIyMDE0NLtbz8lNQQF2fb0ryU1LTMvNQUkJLMtEqX_OSQyoJU27TEnOJUtdSk_PxsFJPiYSYAAGi40aZjAAAAWKE

RUIZ MIGUEL, C., *La configuración constitucional del derecho a la intimidad*, Tecnos, Madrid, 1995

SÁNCHEZ GUARIDO, A., MADDIO MEDINA, A., *"El TJUE reabre el debate entre privacidad o seguridad nacional"*, Diario La Ley, nº. 9743, 2020, pp. 1-5, en https://www.perezllorca.com/wp-content/uploads/2020/11/diario-ley-tjue-reabre-debate-privacidad-seguridad-nacional.pdf

SARMENTO, D., *Poder Judicial e integración europea*. Thomson Civitas, Madrid, 2004

SCHÜNEMANN, B. "*¿Peligros para el estado de derecho a través de la europeización de la administración de justicia penal?"*, en Armenta Deu, T. (Coord), *El Derecho procesal penal en la Unión Europea. Tendencias actuales y perspectivas de futuro*, ed. Colex, 2006, pp. 19-36

SERRA CRISTÓBAL, R., *"Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo. Lo que el constitucionalismo y el derecho de la Unión Europea pueden ofrecer en común"*, UNED, Teoría y Realidad Constitucional, núm. 38, 2016, pp. 487-503.

- *"El impacto de las medidas de seguridad antiterroristas en los derechos fundamentales: La necesidad de normas comunes supranacionales de protección de derechos para responder al riesgo de terrorismo"*, en IX

Congreso Mundial de Derecho Constitucional, Desafíos constitucionales: globales y locales, Oslo, 16-20 de junio de 2014

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

SOBRINO GARCÍA, I., *"Protección de datos y privacidad. Estudio comparado del concepto y su desarrollo entre la Unión Europea y Estados Unidos"*, UNED, Revista de Derecho, núm. 25, 2019, pp. 687-713.

TEJERINA RODRÍGUEZ, O., *Seguridad del Estado y privacidad*, *Edición Reus*, 2014

TOMÁS MALLÉN, B., *"Privacidad versus seguridad en el ámbito europeo"*, en Fayos Gardó, A. y Conde Colmenero, P., *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2014, pp. 215-241

- *"La ejecución de sentencias del Tribunal de Justicia como responsabilidad compartida: luces y sombras"*, Teoría y Realidad Constitucional, UNED, 2017, pp. 449-481

TORRES PÉREZ, A. *Conflicts of Rights in the European Union. A Theory of Supranational Adjudication*, Oxford University Press, Oxford, 2009

TRONCOSO REIGADA, A. *"Hacia un nuevo marco jurídico europeo de la protección de datos personales"*. Revista Española de Derecho Europeo, nº 43, julio-septiembre 2012, pp. 25 a 184

UGARTEMENDIA ECEIZABARRENA, J.I., *"La eficacia entre particulares de la Carta de Derechos Fundamentales de la Unión Europea a la luz de la jurisprudencia del Tribunal de Justicia"*, Teoría y Realidad Constitucional, núm. 39, UNED, 2017, pp. 361-386

VILASAU, M., *"La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad"*, IDP, Revista de Internet, Derecho y Política, núm. 3, UOC, pp. 1-15

WARREN, S.; BRANDEIS, L., *"The right to privacy"*, Harward Law Review (15 de diciembre de 1890), vol. 4, nº. 5

ZAPATER DUQUE, E y PI LLORENS M.., *La dimensión exterior del espacio de libertad, seguridad y justicia*, Marcial Pons, Madrid, 2014

DOCUMENTOS DE CONSULTA

Acuerdo PNR UE-Japón: El Consejo autoriza la apertura de las negociaciones, 18 de febrero de 2020, en https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/?utm_source?dsms-auto&utm_medium=email&utm_campaign=EU-Japan+PNR+agreement%3aCuncil+authorises+opening+of+negotiations

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

Circular 1/2013, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, de la Fiscalía General del Estado, en https://www.boe.es/buscar/abrir_fiscalia.php?=id=FIS-C-2013-00001.pdf

COM (2011) 225 final. Informe de evaluación de la Directiva de Conservación de Datos

COM (2017) 261 final en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0261&from=EN

Comisión Europea (2003) 826 final, de 16 de septiembre de 2003

Comisión Europea (2007) 654 final, de 6 de noviembre de 2007

Comisión Europea (2010) 492 final, de 21 de septiembre de 2010

Comisión Europea (2011) 32 final, de 2 de febrero de 2011

Comisión Europea (2017), Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)", COM (2017) 10 final, Bruselas, 10 de enero de 2017

Comisión Europea (2020) 262 final, de 24 de junio de 2020

Comisión Europea (2020) 264 final, de 24 de junio de 2020

Comisión Europea (2020) 605 final, de 24 de julio de 2020

Comité de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) es una de las Comisiones del Parlamento Europeo, que se encarga de los asuntos legislativos y políticos de mayor relevancia para los ciudadanos europeos en el ámbito de la libertad, seguridad y justicia, según establece el artículo 3 del TUE. https://www.europarl.europa.eu/committees/es/libe/about

Commission Staff Working Document accompanying the Report form the Commission to the European Parliament and the Council, on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection,

investigation and prosecution of terrorist offences and serious crime, COM (2020) 305

Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending ……, en https://delegates.consilium.europa.eu/index.html?targetPath=private/controller/documents:documentSaveAs&docType=ST&docNumber=15119&docQualifier=ADD%202&docYear=2017&language=EN&docFormat=PDF

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2021) 170 final, de 14.4.2021

Comunicación de la Comisión al Consejo y al Parlamento Europeo, Programa de La Haya: diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia", Bruselas, 10.5.2005, COM (2005) 184 final, en http://www.eur-lex.europa.eu/ES/legal-content/summary/the-hague-programme-10-priorities-for-the-next-five-years-html

Comunicación de la Comisión al Parlamento Europeo y al Consejo "La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura", que propone acciones para la implementación de la estrategia durante el periodo 2011-14 (COM/2010/0673 final)

Conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo. Resolución del Parlamento Europeo, de 12 de diciembre de 2018, sobre las conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo (2018/2044(INI)), https://www.europarl.europa.eu/doceo/document/TA-8-2018-0512_ES.pdf

Conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo. Resolución del Parlamento Europeo, de 12 de diciembre de 2018, sobre las conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo (2018/2044(INI)), en https://www.europarl.europa.eu/doceo/document/TA-8-2018-0512_ES.pdf

Consejo de Europa, Protocolo Adicional al Convenio para la protección de las personas con respecto al procesado automático de datos personales en relación con las autoridades de supervisión y los flujos de datos transfronterizos, abierto para su firma en Estrasburgo el 8 de noviembre de 2001, CETS, en: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000001680080626

Consejo de la Unión Europea, en "Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12, 9009/14", Brussels, 5 May 2014, Exchange of views between Commissioner Dimitris Avramopoulos and MEPs at the LIBE Committee

in the European Parliament, 3 December 2014, en http://europa.eu/rapid/pres-release_SPEECH-14-2351_en.htm

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

Coordinating Committee in police and judicial cooperation in criminal matters (CATS), https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/coordinating-committee-area-police-judicial-cooperation-criminal-matters/

Decisión marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros - Declaraciones de algunos Estados miembros con motivo de la adopción de la Decisión marco DO L 190 de 18.7.2002

Decisión Marco del Consejo 2002/475/JAI de 13 de junio de 2002, relativa a la lucha contra el terrorismo, OJ L 164, 22.6.2002, p. 3

Decisión, de 24 de junio de 2014 relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad (2014/415/UE), artículo 8

Declaración conjunta de la Cumbre UE-Canadá, Montreal, 17-18 de julio de 2019

Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo el 25 de marzo de 2004

Dictamen 4/2005, adoptado el 21 de octubre de 2005 (1868/05/ES. WP 113), sobre la Propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM (2005)438 final de 21.09.2005], en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_es.pdf

Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 20 de junio

Dictamen del Comité Económico y Social Europeo, de 19 de enero de 2006, sobre la "Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE" COM (2005) 438 final – 2005/0182 (COD). (2006/C 69/04). DO C 69 de 21.3.2006, en http://eur-lex.europa.eu/LexUriServ/site/es/oj/2006/c_069/c_06920060321es00160021.pdf

Dictamen del SEPD, adoptado el 26 de septiembre de 2005 (2005/C 298/01), sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final], DO C 298 de 29.11.2005 en: http://eur-lex.europa.eu/LexUriServ/site/es/oj/2005/c_298/c_29820051129es00010012.pdf

Dictamen del Servicio Jurídico de 20 de junio de 2001 (doc. 10146/01, de la Secretaría General del Consejo)

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril, 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 del Consejo 2008/977/JAI

Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se deroga la Decisión Marco 2002/475/JAI y se modifica la Decisión del Consejo 2005/671/JAI, OJ L 88, 31.3.2017

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)

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

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

Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, OJ L24, 30.01.1998, en: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN

Documento 5840/21 del Consejo de la Unión Europea, que contiene la orientación general de esta institución europea respecto del borrador de Reglamento del Parlamento Europeo y del Consejo relativo al respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas y por la que se deroga la Directiva 2002/58/CE (Reglamento de privacidad y las comunicaciones electrónicas).

Documento 6087/21 del Consejo de la Unión Europea, que contiene el enfoque general de esta institución europea respecto del borrador de Reglamento de privacidad de las comunicaciones electrónicas

Documento 9802/17 de la Secretaría General del Consejo

Documento SN 18/21, de 25 de marzo de 2021, https://www.consilium.europa.eu/media/49007/250321-vtc-euco-statement-es-pdf

Estrategia de la UE para la Unión de la Seguridad, P9_TA(2020)0378, consultada el 14.04.21 en https://www.europarl.europa.eu/doceo/document/TA-9-2020-0378_ES.pdf. Letra M

EUCO 22/20, consultado en https://www.consilium.europa.eu/media/47348/1011-12-20-euco-conclusions-es-pdf

EUROJUST, EJCN, https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network

European Data Protection Supervisor (EDPS), "Reflection paper of the European Data Protection Supervisor on the interoperability of information systems in the area of Freedom, Security and Justice", 17 November 2017, en https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf

European Union Agency for Fundamental Rights, "Fundamental Rights Report 2018", ISBN 978-92-9491-928-1 en http://fra.europa.eu/en/publicatin/2018/fundamental-rights-report-2018

Europol, Data Protection Office. EDOC#791813 (Study on the Data Retention Regime Applied in the EU Member States)

EUROPOL, EC3, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Factsheet -Personal Data Protection, 2018, del Consejo de Europa, disponible en: https://www.coe.int/en/web/data-protection/echr-case-law

Fiscalía Europea https://www.consilium.europa.eu/es/policies/eppo/

Guía de Necesidades del SEPD, en https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

Guía práctica del procedimiento legislativo ordinario", manual sobre la labor del Parlamento Europeo como colegislador, septiembre de 2020, Bruselas, PE 640,179, en https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/handbook-on-the-ordinary-legislative-procedure

Hessisches Datenschutzgesetz (Ley de Protección de Datos del Land de Hesse) 1970, en vigor desde el 13 de octubre de 1970, B.O.E del Land, Parte I, 1970, Nr. 41 (12 de octubre de 1970), disponible en: https://starweb.Hesse.de/cache/GVBL/1970/00041.pdf

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

Informe de la Agencia ENISA: "Data pseudonymisation: advanced techniques and use cases. Technical análisis of cibersecurity measures in data protectin and privacy", January 2021, DOI 10.2824/860099, https://www.enisa.europa,eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

Informe de la Oficina del Alto Comisionado para los Derechos Humanos del Consejo de Derechos Humanos (CDH) de las Naciones Unidas, sobre el derecho a la privacidad en la era digital, de 30 de junio de 2014, A/HRC/27/37, nº. 19

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Manual del Delegado de Protección de Datos, guía para los delegados de protección de datos en los sectores públicos y semipúblicos sobre cómo garantizar el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea, elaborado para el proyecto "T4DATA" financiado por la UE, en https://www.aepd.es/sites/default/files/2019-12/El%20Manual/%2del%20DPD%/20-%20KORFFGEORGES%20-%ESP.pdf

Manual de legislación europea en materia de protección de datos, edición 2018, Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2019

Naciones Unidas, Guía para la regulación de los ficheros automatizados de datos personales, UNGA Res. 44/132, 44 UN GAOR Supp. (Nº. 49) en 211, UN Doc. A/44/49 (1989), en https://www1.umn.edu/humanrts/instree/q2grcpd.htm

Nota del Servicio Jurídico del Consejo al COREPER (doc.5884/17)

OCDE, Recomendaciones del Consejo acerca de las Guías que rigen la Protección de la Privacidad y el flujo transfronterizo de datos personales, de 23 de septiembre de 1989, en: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtrnasborderflowofpersonal_data.htm

Privacy International (2017). National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, September 2017

Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano", aprobado por el Consejo de Justicia y Asuntos de Interior el 1 de diciembre de 2009, en https://eur-lex.europa.eu/ES/legal-content/summary/the-stockhom-programme.html

Propuesta de Directiva del Parlamento Europeo y del Consejo estableciendo reglas armonizadas sobre el nombramiento de representantes legales para la recogida de pruebas en procedimientos

Propuesta de la Comisión para una Directiva del Parlamento Europeo y del Consejo sobre la retención de información procesada en relación con la provisión de los

servicios de comunicación electrónica pública y por la que se modifica la Directiva 2002/58/EC, COM (2005) 438 final, 21 de septiembre de 2005

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (fronteras y visados) y por el que se modifican la Decisión 2004/512/CE del Consejo, el Reglamento (CE) nº. 767/2008, la Decisión 2008/633/JAI del Consejo, el Reglamento (UE) 2016/399 y el Reglamento (UE) 2017/2226, en http://delegates.consilium.europa.eu/index.html?targetPath=private/controller/documents:documentSaveAs&docType=ST&docNumber=15119&docQualifier=INIT&docYear=2017&language=ES&docFormat=PDF

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (cooperación policial y judicial, asilo y migración), COM (2017) 784 final, en https://delegates.consilium,europa.eu/index.html?targetPath=private/controller/documents:documentSaveAs&docType=ST&docNumber=15729docQualifier=INIT&docYear=2017&language=ES&docFormat=PDF

Propuesta de reglamento del Parlamento y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a los efectos de enjuiciamiento penal COM (2018) 0108 (COD), https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0006.02/DOC_2&format=PDF

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 el suministro de datos en redes públicas de comunicaciones a efectos de la prevención, investigación, descubrimiento y represión de la delincuencia y de las infracciones penales, con inclusión del terrorismo, presentada por la República Frances, Irlanda, el Reino Unido y el Reino de Suecia, el 28 de abril de 2004 (CNS/2004/0813), en http://register.consilium.eu/int/pdf/es/04/st08/st08958.es04.pdf

Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso

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

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismo de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento

(CE) nº. 45/2001 y la Decisión nº. 1247/2002/CE, OJ L 295, 21.11.2018, p. 39-98, en http://data.europa.eu/eli/reg/2018/1725/oj

Reglamento (UE) 2019/817 del Parlamento y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) nº. 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, OJ L 135, 22.5.2019, p-27-84, en http://data.europa.eu/eli/reg/2019/817/oj

Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816, OJ L 135, 22.5.2019, p. 85-135, en http://data.europa.eu/eli/reg/2019/818/oj

Resolución 2396 (2017), adoptada por el Consejo de Seguridad en su reunión 8148, de 21 de diciembre de 2017

Resolución del Consejo de Europa 1974 (74)29 sobre Protección de la privacidad de las personas frente a los bancos de datos electrónicos en el sector público, en https://www.oecd.org/sti/iconomy/oecdguidelinesonttheprotectionofprivacyandtransborderflowsofpersonal_data.htm

Resolución del Consejo de Europa de 1973 (73)22 sobre Protección de la privacidad de las personas frente a los bancos electrónicos en el sector privado, en https://rm.coe.int/CoERMPbulicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830

Resolución del Parlamento, de 15 de diciembre de 2005, sobre la presunta utilización de países europeos, por parte de la CIA, para el transporte y la detención ilegal de presos (DO C 286 E de 23.11.2006, p. 509)

Situación de los derechos fundamentales en la Unión Europea: informe anual para los años 2018 y 2019. P9_TA(2020)0328, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0328_ES.pdf

Supervisor Europeo de Protección de Datos (2017), "Herramientas para determinar la necesidad", https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf

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

Tratado de la Unión Europea, de 7 de febrero de 1992, firmado en Maastricht (conocido por ese nombre, al que ya nos hemos referido en párrafos precedentes a esa nota), publicado en el DOUEC núm. 340, de 10 de noviembre de 1997, vigente desde el 1 de mayo de 1999 y revisión vigente desde el 1 de septiembre de 2016, en https://noticias.juridicas.com/base_datos/Admin/tue.html

Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea (2007/C 306/01), publicado el 17 de diciembre de 2007, en https://www.boe.es/doue/2007/306/Z00001-00271.pdf

WK 11460/2020 INIT, Study on the retention of electronic communications non-content data for law enforcement purposes, final report, de 22 de octubre de 2022

JURISPRUDENCIA

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

Conclusiones del Abogado General Sr. Henrik Saugmandsgaard Oc. De 19 de julio de 2016, en los Asuntos acumulados C-203/15 y C-698/15, Tele 2 Sverige AB contra Post- och telestyrelsen (C-203/15) y Secretary of State for the Home Department contra Tom Watson, Peter Brice, Geoffrey Lewis

Dictamen 1/15 del Tribunal de Justicia (Gran Sala), ECLI:EU:C:2017:592

Sentencia de 9 de enero de 2001 (1 BvR 1036/99). EuZW 2001, p. 256 (255), el Tribunal Constitucional alemán

Sentencia del TEDH de 2 de agosto de 1984, Caso Malone

Sentencia del TEDH de 24 de febrero de 1998, Caso Botta c. Italia

Sentencia del TEDH, de 16 de diciembre de 1992, Caso Niemietz contra Alemania

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

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

Sentencia del TJUE, de 20 de diciembre de 2017, asunto C-434/16, Peter Nowak y Data Protection Commissioner, ap. 31 y Sentencia TJUE, de 19 de octubre de 2016, asunto C-582/14, Patrick Breyer y Bundesrepublik Deutschland

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

Sentencia del Tribunal de Justicia (Gran Sala), de 13 de mayo de 2014, en el asunto C-131/12

Sentencia del Tribunal de Justicia (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14

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

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

Sentencia TEDH de 25 de junio de 1997, ECtHR, Halford v. el Reino Unido

Sentencia TEDH, Copland contra Reino Unido, 3.4.2007

Sentencia TEDH, de 25 de mayo de 2021, Big Brother Watch y otros c. Reino Unido (CE:ECHR:2021:0525JUD 005817013), y de 25 de mayo de 2021, Centrum för Rättvisa c. Suecia (CE:ECHR:2021:0525JUD 003535208)

Sentencia TEDH, Marper contra Reino Unido, 4.12.2008

Sentencia TEDH, Von Hannover contra Alemania (nº 2), números 40660/08 y 60641/08, de 7 de febrero de 2012; TJUE, asuntos acumulados C-468/10 y C-469/10

Sentencia TJUE (Gran Sala) Personal Name Records, asuntos acumulados C-371/04 y C-318/04, de 30 de agosto de 2006

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

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

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

Sentencia TJUE (Sala Primera), de 18 de enero de 2007, en el asunto C-229/05 P, que tiene por objeto un recurso de casación interpuesto con arreglo al artículo 56 del Estatuto del Tribunal de Justicia, 2l 9 de mayo de 2005

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

Sentencia TJUE de 15 de julio de 1964, Costa, 6/64, EU:C:1964:66, pp. 105 y 106; de 19 de noviembre de 2019; A.K. y otros (Independencia de la Sala Disciplinaria del Tribunal Supremo)

Sentencia TJUE de 17 de diciembre de 2020, Centraal Israëlitisch Consistorie van België y otros, C-336/19

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

Sentencia TJUE en el asunto C-817/19 Ligue des droits humains, Luxemburgo, 21 de junio de 2022

Sentencia TJUE en los casos C-317/04 y C-318/04, Parlamento Europeo contra Consejo y Comisión, de 30 de mayo de 2006

Sentencia TJUE, C-244/80, Pasquale Foglia contra Mariella Novello (nº 2), 16 de diciembre de 1981; TJUE, C-467/04, Procedimiento penal entablado contra Gasparini y otros, 28 de septiembre de 2006

Sentencia TJUE, C-438/05, International Transport Workers' Federation y Finninsh Seamen's Union contra Viking Line ABP y OÜ Viking Line Eesti, 11 de diciembre de 2007

Sentencia TJUE, Caso Rechnungsfof contra Österreichischer Rundfunk y otros, y Christa Neukomm y Jospeh Lauermann vs. Österreichischeer Rundfunk, en Sentencia de 20 de mayo de 2003

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

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

Sentencias TJUE en casos C-27/09 P República Francesa vs. OMPI, 2011 y C-300/11 ZZ vs. Secretario de Estado del Ministerio del Interior, 2013

STS 400/2017, de 1 de junio de 2017

STS 723/2018, de 23 de enero de 2019

STS 727/2020, de 23 de marzo de 2021, recurso de casación núm. 4218/2018

OTROS DOCUMENTOS

Declaración de John Abbott, C.B.E, QPM. B.A. (Hons), antiguo director general del Servicio Nacional de Inteligencia Criminal, Reino Unido, en la primera sesión plenaria del Foro de la Unión Europea sobre Ciberdelincuencia.

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

"Encuesta sobre la protección de datos personales", Teoría y Realidad Constitucional, 46, 2020, pp. 15-118, p. 29, en https://www-proquest-com.bibliotecauned.idm.oclc.org/scholarly-journals/encuesta-sobre-la-protección-de-datos-personales/docview/2535570794/se-2

INCIBE, sobre inteligencia de fuentes abiertas https://www.incibe-cert.es/blog/osint-la-informacion-es-poder.