LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS SOLICITANTES DE PROTECCIÓN INTERNACIONAL EN EL (NUEVO) SISTEMA EUROPEO COMÚN DE ASILO: GRANDES DESAFÍOS Y GRAVES DEFICIENCIAS*

ROSARIO GARCÍA MAHAMUT
Catedrática de Derecho Constitucional
Universitat Jaume I

JORGE VIGURI CORDERO
Investigador de la Universitat Jaume I

Sumario

I. El estado de la cuestión y los grandes retos de la UE en la defensa de los derechos. II. La reforma integral del SECA: claves de la reforma. III. Una primera aproximación al marco jurídico regulador del derecho a la protección de datos de los solicitantes de protección internacional. IV. Seguridad y protección de datos en el vigente Reglamento de Dublín III y la derogada Directiva 95/46/CE. V. El RGPD y su impacto en las propuestas de reforma del SECA. VI. Reflexiones conclusivas.

I. EL ESTADO DE LA CUESTIÓN Y LOS GRANDES RETOS DE LA UE EN LA DEFENSA DE LOS DERECHOS

La grave crisis migratoria y de refugiados que se produjo entre los años 2014 a 2017, y que se cobró trágicamente la vida de cientos de miles de personas en el Mediterráneo tratando de arribar a Europa, ha marcado un antes y un después en la Política Europea de Migración y Asilo y en los distintos instrumentos normativos que se activaron para solventar las lagunas y deficiencias que evidenció muy

* El presente trabajo se ha elaborado en el marco de los proyectos RTI2018-095367-B-I00 y AICO/2019/205.

particularmente el Sistema Europeo Común de Asilo (SECA) y, más concretamente, el sistema de Dublín que, a pesar de su reforma del 2013, mostró un alto grado de ineficiencia para hacer frente a situaciones en las que los sistemas nacionales de asilo se enfrentaban a una presión desproporcionada.

Asistimos atónitos a una gravísima emergencia humanitaria que desbordaba día a día a países que, como Italia y especialmente Grecia, asumían en escalada un sobresfuerzo de sus sistemas nacionales tratando de canalizar la llegada masiva de personas traficadas por delincuentes sin escrúpulos, muchas de ellas en clara y manifiesta necesidad de protección internacional (refugio o protección subsidiaria).

Entre otras consecuencias, se hizo patente la necesidad de abordar en Europa una reforma integral del SECA que funcionara de forma eficaz y eficiente, no solo en situaciones de normalidad sino también ante la llegada descontrolada y a gran escala de personas, haciendo viable el cumplimiento de las garantías del ejercicio de los derechos que lleva aparejada la solicitud y, en su caso, el reconocimiento a la protección internacional en la UE.

Pero no solo, el incumplimiento por parte de los Estados de la normativa comunitaria, así como el cierre de fronteras interiores evidenció que la competencia nacional en materia de defensa de la seguridad del Estado era esgrimida por muchos de los Estados miembros (EEMM) como la clave de bóveda para eludir el incumplimiento de la normativa comunitaria en materia del SECA. No obstante, no cabe negar que, ciertamente, el origen de los países de procedencia de las personas que llegaban huyendo de la guerra de Siria, Irak, Afganistán o Pakistán, así como de las mafias que las traficaban con refugiados no solamente evidenció un SECA que hizo agua por los cuatro costados, sino que, incluso, la ineficiencia e ineficacia en la aplicación del mismo derivó, en ocasiones, en un problema para la seguridad de los Estados[1]. De hecho, la Agenda Europea de Seguridad puso el énfasis en la necesidad de establecer estrictas normas comunes de gestión de las fronteras como instrumentos esenciales para prevenir la delincuencia y el terrorismo transfronterizo[2].

La gestión de la información de la UE se reveló como un nudo gordiano para proteger las fronteras exteriores, mejorar la gestión de los flujos migratorios y contribuir a reforzar la seguridad interior. De hecho, la Comisión Europea (CE) en su Comunicación de 6 de abril de 2016 sobre «Sistemas de información más sólidos

1 Lo que sin duda ha ido en detrimento del derecho efectivo a la protección internacional que persigue el propio SECA, entre otras razones, por la incapacidad de asumir ingentes cantidades de solicitudes de protección internacional concentradas, especialmente, en Italia y Grecia, a la par de la imposibilidad de actuar con celeridad para distinguir quienes estaban en necesidad de protección internacional frente a quienes podían constituir una amenaza para la seguridad nacional. Ello, siendo plenamente conscientes que se ha producido, efectivamente, situaciones en la que la seguridad de los Estados se ha podido ver comprometida. Dada la imposibilidad de detenernos sobre el particular, remitimos a Viguri Cordero, J., «La seguridad nacional y la excepción en el Sistema Europeo Común de Asilo (SECA)», *Revista de Derecho Político*, 2019, (pendiente de publicación).

2 COM(2015) 185 final.

e inteligentes para la gestión de las fronteras y la seguridad» activó un proceso de discusión destinado a lograr la interoperabilidad de los sistemas de información de la UE para mejorar la gestión de las fronteras, la migración y la seguridad interior con el objetivo de solucionar las deficiencias estructurales relacionadas con tales sistemas y así garantizar que los guardias de fronteras, las autoridades aduaneras, los agentes de policía y las autoridades judiciales tuvieran a su disposición la información necesaria.

Si en un principio el objetivo de la comunicación fue abrir un debate sobre cómo podían los sistemas de información de la Unión Europea mejorar la gestión de las fronteras y la seguridad, lo cierto es que la CE[3] terminó proponiendo un nuevo enfoque para que la gestión de los datos de los sistemas centralizados de información de la UE a gran escala fueran interoperables, estableciendo un marco para garantizar dicha interoperabilidad en los ámbitos del control fronterizo, el asilo y la inmigración, la cooperación policial y la cooperación judicial en materia penal[4]. Ello se concretó, a instancias del Consejo Europeo[5], en 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) 767/2008, la Decisión 2008/633/JAI del Consejo, el Reglamento (UE) 2016/399 y el Reglamento (UE) 2017/2226[6] y en 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)[7], ambas de 12 de diciembre de 2017.

Tales propuestas legislativas constituyen hoy Reglamentos en vigor[8], aplicables en los términos recogidos en los arts. 75 y 79 de los respectivos Regla-

3 Apoyándose en las recomendaciones del Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad que se constituyó para abordar los retos jurídicos, técnicos y operativos que planteaba la interoperabilidad de los sistemas centrales de la UE para las fronteras y la seguridad. Pueden consultarse el informe provisional presentado en diciembre de 2016 y el informe final, de 11 de mayo de 2017, en https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435&Lang=ES. Debe destacarse que la Agencia Europea de los Derechos Fundamentales, el Supervisor Europeo de Protección de Datos y el Coordinador de la lucha contra el Terrorismo de la UE participaron activamente en los trabajos del Grupo de Expertos. Para una comprensión global del contexto debe tenerse presente la Resolución del Parlamento Europeo, de 6 de julio de 2016, sobre las prioridades estratégicas para el programa de trabajo de la Comisión para 2017 [2016/2773 (RSP)].

4 Véase la Comunicación de la Comisión, de 16 de mayo de 2017, al Parlamento Europeo, al Consejo Europeo y al Consejo, Séptimo informe de situación hacia una Unión de la Seguridad genuina y efectiva, COM(2017) 261 final.

5 Véase las Conclusiones del Consejo sobre las vías de avance para mejorar el intercambio de información y garantizar la interoperabilidad de los sistemas de información de la UE http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/es/pdf

6 COM(2017)793 final, 12.12.2017.

7 COM(2017)794 final, 12.12.2017. Para consultar la propuesta modificada véase COM(2018)0480.

8 Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo de 20 de mayo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de

mentos. Y, para dar buena cuenta de la magnitud y del impacto que ambos van a tener de futuro, solo basta reproducir el Considerando 8, idéntico, de ambos Reglamentos:

«Con objeto de mejorar la efectividad y la eficiencia de las inspecciones en las fronteras exteriores, contribuir a prevenir y combatir la inmigración ilegal y alcanzar un elevado nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión, lo que incluye el mantenimiento de la seguridad pública y del orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros, mejorar la aplicación de la política común de visados y prestar asistencia en el examen de las solicitudes de protección internacional y en la prevención, detección e investigación de los delitos de terrorismo u otros delitos graves, ayudar a identificar a las personas desconocidas que no puedan identificarse o los restos humanos sin identificar en caso de catástrofes naturales, accidentes o atentados terroristas, con el fin de mantener la confianza de los ciudadanos en la política de migración y el sistema de asilo de la Unión, en las medidas de seguridad de la Unión y en las capacidades de la Unión en materia de gestión de las fronteras exteriores, *debe establecerse la interoperabilidad de los sistemas de información de la U*E, es decir el Sistema de Entradas y Salidas (SES), el Sistema de Información de Visados (VIS), el Sistema Europeo de Información y Autorización de Viajes (SEIAV), Eurodac, el Sistema de Información de Schengen (SIS), y el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN), *para que estos sistemas de información y sus datos se complementen mutuamente, respetando al mismo tiempo los derechos fundamentales de los individuos, especialmente el derecho a la protección de los datos personales*. Para ello, deben crearse, como componentes de interoperabilidad, un portal europeo de búsqueda (PEB), un servicio de correspondencia biométrica compartido (SCB compartido), un registro común de datos de identidad (RCDI) y un detector de identidades múltiples (DIM)».

La interoperabilidad de los sistemas de información de la UE debe permitirles complementarse a fin de facilitar la identificación correcta de las personas, tal y como expresamente prevé el Considerando 9, «contribuir a luchar contra la usurpación de identidad, mejorar y armonizar los requisitos de calidad de los datos de los respectivos sistemas de información de la UE, facilitar la aplicación técnica y operativa por los Estados miembros de los sistemas de información de la UE, reforzar las garantías de seguridad de los datos y de protección de datos que rigen en los respectivos sistemas de información de la UE, racionalizar el

las fronteras y los visados y por el que se modifican los Reglamentos (CE) n. 767/2008, (UE) 2016/399, (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 y el Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo de 20 de mayo 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.

acceso con fines de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves al SES, el VIS, el SEIAV Eurodac, y apoyar los objetivos del SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN».

Innumerables, poliédricos y de profundo calado han sido los desafíos que tal escenario ha planteado desde el minuto cero a la UE y cuyas consecuencias seguirán condicionando, a medio y a largo plazo, las políticas y la acción legislativa de la misma y la de los EEMM. Recuérdese que, como ya analizamos en otro lugar[9], esa crisis y emergencia humanitaria sin parangón exigió acciones inmediatas de todo orden —incluidas la normativa de urgencia de carácter provisional en su respuesta tardía a la crisis por parte de la UE—, la revisión de las políticas públicas (incluidas las de seguridad) y toda una agenda de modificaciones legislativas, lo que a nuestro juicio, ya no permite hablar de una nueva fase en el desarrollo del SECA sino de un «nuevo SECA», tal y como analizaremos con posterioridad.

De entre todos los desafíos, se ha transparentado uno que, en el ámbito del derecho a la protección internacional, comenzó a demandar hace ya algún tiempo atención por parte de la doctrina y es, precisamente, el que afecta al tratamiento de los datos personales de los solicitantes de asilo y protección subsidiaria.

La práctica ausencia, no solamente en España sino en la UE, de estudios, análisis y reflexiones sobre la materia en el contexto de un mundo absolutamente en línea resulta una exigencia inmediata y obligada para la doctrina, dado los conflictos constitucionales de derechos fundamentales en juego —el de la protección de los datos personales en el ámbito de la protección internacional— y las graves implicaciones que revisten en un ecosistema normativo multinivel; plagado de incertidumbres jurídicas en cuanto al marco jurídico de aplicación, a las reservas competenciales y al sistema de garantías y limitaciones de los derechos en juego en diversos escenarios condicionados por los accesos y diversos controles a las fronteras exteriores de la UE a lo que deberá sumarse los mandatos del paquete de interoperabilidad.

Sin duda, nos enfrentamos a una enorme complejidad normativa que, metodológicamente, exigirá aproximarnos desde distintas perspectivas —y diversas variables—, pero en un contexto delimitado: la propuesta de reforma del SECA y los desafíos que se plantean al tratamiento de los datos personales que, a su vez, exige delimitar su régimen jurídico, especialmente, cuando interacciona con la seguridad de los EEMM.

En esta línea, no podemos perder de vista que los nuevos retos a los que se enfrenta la migración y asilo en la UE y las continuas implicaciones también para la seguridad de los EEMM exige crear registros e investigaciones cada vez más completos y exactos. La determinación fehaciente de las personas merecedores del

9 García Mahamut, R., «La ductilidad del derecho a la protección internacional (refugio y protección subsidiaria) ante las crisis humanitarias: un desafío para Europa y para el Sistema Común de Asilo» *Teoría y Realidad Constitucional*, n.º 38, 2016, pp. 225 a 232.

pleno derecho a protección internacional exige, a día de hoy, identificar exhaustivamente el perfil del solicitante con objeto de diferenciarlo, sin ningún género de duda, de otras categorías de sujetos —y que abarca no solo a migrantes sino también a potenciales delincuentes y/o terroristas—.

Esta situación ha favorecido la creación de nuevas iniciativas tendentes a garantizar que las autoridades de los Estados conozcan en detalle quién cruza las fronteras exteriores comunes de la UE. Como ya hemos precisado, se ha abogado por el establecimiento de sistemas de información interoperables y por la gestión exhaustiva de las fronteras interiores y exteriores para reforzar los instrumentos que ponen en riesgo la seguridad europea y, en coherencia con ello, reforzar y racionalizar las condiciones de seguridad y protección de datos que rigen los respectivos sistemas así como mejorar y armonizar los requisitos de calidad de los datos de esos sistemas.

No en vano, a finales de 2018, la CE destacó la exigencia de garantizar el respeto de las nuevas leyes de seguridad así como de la protección de datos en el ámbito del asilo[10]. Derecho a la protección de los datos personales cuyo ejercicio se conjuga con las limitaciones y garantías que proporcionan otros instrumentos jurídicos de enorme envergadura como lo es, entre otros, el Reglamento General de Protección de Datos (RGPD)[11] directamente aplicable en todos los Estados de la UE desde mayo de 2018 y la Directiva (UE) 2016/680 de protección de datos en el ámbito policial y de justicia.[12]

Un régimen jurídico que, como abordaremos más adelante, resulta especialmente complejo en el SECA y que se agrava por todo un conjunto de organismos y agencias que operan directa o indirectamente en el tratamiento de las solicitudes de protección internacional. Por un lado, el tratamiento de datos personales por parte de instituciones, órganos y organismos de la Unión se encuentra regulado por el Reglamento (UE) 2018/1725[13], que se aplica directamente a los organismos y agencias especializadas que operan en las solicitudes de protección internacional como la Guardia Europea de Fronteras y Costas (FRONTEX)[14] o la futura Agencia

10 Comisión Europea, *Una Europa que protege: la Comisión pide un mayor esfuerzo para garantizar la adopción de las propuestas sobre seguridad,* 11 de diciembre de 2018.

11 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, pp. 1–88).

12 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, pp. 89–131).

13 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 organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DOUE de 21 de noviembre de 2018).

14 Propuesta de Reglamento sobre la Guardia Europea de Fronteras y Costas —y por el que se derogan la Acción Común n.º 98/700/JAI del Consejo, el Reglamento (UE) n.º 1052/2013 del Parlamento Europeo y

de Asilo de la UE —que viene a sustituir a la Oficina Europea de Apoyo al Asilo—.[15] Por otro lado, toda la normativa europea reguladora de aquellas bases de datos y sistemas de información específicos a través de las cuales se obtienen, tratan, almacenan e intercambian datos personales altamente sensibles puestos al servicio de la Seguridad de las personas, de la seguridad en las fronteras, de la seguridad de los EEMM, y por ende de la UE y, cómo no, para el funcionamiento eficiente y eficaz del SECA. Todo ello aderezado por la incertidumbre jurídica que arroja sobre numerosos ámbitos del ejercicio de los derechos los reglamentos de interoperabilidad, entre otras cuestiones, por afectar a bases de datos que se encuentran en fase de negociación o reforma, entre ellas Eurodac, piedra angular en esta materia del SECA. Estatuto de refugiado o protección subsidiara cuya razón misma de ser no es otra que garantizar a un nacional de un tercer país que debido a fundados temores de ser perseguido por motivos de raza, religión, nacionalidad, opiniones políticas o pertenencia a determinado grupo social, o que se encuentra fuera del país de su nacionalidad y, no puede o, a causa de dichos temores, no quiere acogerse a tal protección, poder obtener dicha protección. En consecuencia, hablamos de datos absolutamente confidenciales y especialmente protegidos al objeto de que los países frente a los que se otorga protección a sus nacionales no puedan acceder a los mismos.

II. LA REFORMA INTEGRAL DEL SECA: CLAVES DE LA REFORMA

En este apartado abordaremos de forma sinóptica el porqué, el cómo y la hoja de ruta de la renovación de las bases legales del SECA tras el anuncio de la CE, el 6 de abril de 2016[16], al objeto de poder, con posterioridad, deslindar aquellos aspectos que cambian conceptualmente al asumir la UE que los retos que afectan a la seguridad común en la UE debe ser abordados de forma colectiva y común por los EEMM.

del Consejo y el Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo Contribución de la Comisión Europea— (COM (2018) 0631 —C8-0406/2018— 2018/0330(COD)), de 12 de febrero de 2019. El 12 de septiembre de 2018, la CE propuso la actualización del Reglamento de la Guardia Europea de Fronteras y Costas con el objetivo de mejorar el control de las fronteras exteriores de la UE. Esta Propuesta fue confirmada por el Consejo el pasado 1 de abril de 2019.

15 Propuesta enmendada de Reglamento relativo a la Agencia de Asilo de la Unión Europea y por el que se deroga el Reglamento (UE) n.º 439/2010, Bruselas, 12 de septiembre de 2018COM (2018) 633 final 2016/0131 (COD). A fecha de elaboración del presente trabajo, la situación sobre la propuesta es la siguiente: el 23 de enero de 2019, la Presidencia del Consejo presentó la propuesta modificada al Coreper en el que se subrayó que las propuestas de la Presidencia no contaban con el apoyo suficiente. El 4 de febrero, la Presidencia convocó una reunión de los Consejeros JAI, en la que fue examinado el nuevo texto. Sin embargo, puesto que no hubo cambios significativos en la posición de los Estados miembros con respecto a la reunión anterior, la Presidencia concluyó que se habían agotado todas las posibilidades a nivel técnico.

16 «Hacia una reforma del Sistema Europeo Común de Asilo y una mejora de las vías legales de entrada en Europa», COM(2016) 197 final.

Si algo puso de relieve la gravísima emergencia humanitaria, como ya precisamos, es que ese «espacio común de protección y solidaridad fundado en un procedimiento común de asilo y un estatuto uniforme para las personas a las que se concede protección internacional basado en normas de protección de alto nivel y unos procedimientos justos y eficaces» hizo aguas cuando las avalanchas migratorias se concentraron en determinados Estados, no pudiendo responder el sistema nacional de asilo del Estado afectado a la exigencia ineludible del objetivo que persigue el SECA, esto es, «que las personas, independientemente del Estado miembro en que se presente su solicitud de protección internacional, deben recibir el mismo nivel de tratamiento en lo referente a la tramitación del procedimiento y la determinación del estatuto».

A pesar, incluso, de la activación de mecanismos jurídicos dentro de la UE para hacerles frente, lo cierto es que, como ya hemos analizado en otro lugar[17], fueron numerosos los Estados que obstaculizaron en nombre de la seguridad la aplicación de tales medidas y, desde luego, no actuaron con la responsabilidad, diligencia y rapidez necesarias reubicando y reasentando a las personas en necesidad de protección internacional en el número correspondiente y en el plazo fijado en las distintas Decisiones jurídicamente vinculantes adoptadas en la UE. No solo se incumplió por parte de muchos EEMM ese reparto de responsabilidades más justo que hiciera del SECA un sistema más equitativo, eficiente y sostenible, sino que, incluso, algunos cerraron sus fronteras interiores. Los procedimientos se volvieron laxos, los EEMM aducían problemas de seguridad y los distintos datos personales de los migrantes no se gestionaban con la exigencia y celeridad que requería la tramitación del procedimiento de asilo y, devoluciones, en su caso.

Esta situación dejó patente la necesidad en Europa de una reforma integral del SECA «capaz de garantizar un reparto de responsabilidades justo y sostenible entre los Estados miembros, de ofrecer unas condiciones de acogida suficientes y decentes en todo el territorio de la UE, de tramitar rápida y eficazmente las solicitudes de asilo presentadas en la UE y de asegurar la calidad de las resoluciones que se dictan de modo que las personas que necesiten protección internacional puedan conseguirla de forma efectiva» como prevé la propuesta de Reglamento por la que se establece un procedimiento común.

Para cumplir tales objetivos, la CE en plena crisis esbozó los distintos pasos que debían darse hacia una política de asilo más humana, justa y eficaz a la vez que para una política de migración legal mejor gestionada. Esta hoja de ruta se concretaba en un primer conjunto de propuestas para reformar el SECA y un segundo paquete integrado por la aprobación de reformas legislativas adicionales que pretenden reformar el acervo del asilo propiciando un sistema sólido,

17 García Mahamut, R., «La ductilidad del derecho a la protección internacional…, *op. cit,* p. 211-238.

coherente e integrado, basado en normas comunes y *armonizadas*, eficaces y protectoras que completa esa reforma del SECA.

Entre las que se incluye dentro del primer tramo de reformas legislativas destacan: la propuesta de reforma del actual Reglamento de Dublín III (PRD IV)[18], la propuesta de refundición del Reglamento Eurodac —convirtiéndose este también en una base de datos para objetivos más generales relacionados con la inmigración (retorno y lucha contra la migración irregular)–[19] y la propuesta de creación de una Agencia de Asilo de la UE[20] que facilitase el funcionamiento del SECA, garantizando la convergencia en la evaluación de las solicitudes de protección internacional en toda la UE, y la que corresponderá realizar un seguimiento operativo y técnico de la aplicación del Derecho de la Unión.

La segunda fase está integrada por la presentación de propuestas legislativas cuyo objetivo es reformar y sustituir la Directiva sobre procedimientos por un Reglamento[21] que armoniza los distintos requisitos procedimentales en los EEMM creando un procedimiento común. En la misma línea, también sustituye por un Reglamento la Directiva sobre los requisitos para el reconocimiento[22] de las personas en necesidad de protección internacional, así como de los derechos

18 Propuesta de Reglamento por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida (texto refundido). COM/2016/0270 final — 2016/0133 (COD). A fecha de elaboración del presente trabajo, la situación sobre la propuesta es la siguiente: en junio de 2018, el Consejo Europeo concluyó que debía conseguirse un consenso sobre el Reglamento de Dublín. Un debate que, a día de hoy, continúa.

19 Propuesta de Reglamento relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del [Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida] y de la identificación de un nacional de un tercer país o un apátrida en situación ilegal, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley (refundición) COM/2016/0272 final — 2016/0132 (COD). A fecha de redacción del presente artículo, la situación sobre la propuesta es la siguiente: el 14 de febrero de 2018, el Coreper amplió el mandato de negociación del Consejo en relación con el Reglamento Eurodac incluyendo asimismo cuestiones relacionadas con el reasentamiento. Posteriormente, la Presidencia del Consejo convocó una reunión de los Consejeros JAI el 25 de febrero de 2019 en la que presentó la última propuesta transaccional del Parlamento Europeo. Aunque los Estados miembros acogieron favorablemente la última propuesta del Parlamento, no encomendaron a la Presidencia que continuara las negociaciones.

20 Propuesta enmendada de Reglamento relativo a la Agencia de Asilo de la Unión Europea, *op. cit.*

21 Propuesta de Reglamento por el que se establece un procedimiento común en materia de protección internacional en la Unión y se deroga la Directiva 2013/32/UE (COM/2016/0467 final — 2016/0224 (COD). A fecha de redacción del presente artículo, la situación sobre la propuesta es la siguiente: en marzo de 2019, los Consejeros JAI remitieron al Coreper el expediente con los progresos realizados para avanzar hacia una versión consolidada, a día de hoy, pendiente de obtener orientaciones adicionales.

22 Reglamento por el que se establecen normas relativas a los requisitos para el reconocimiento de nacionales de terceros países (COM (2016) 466 final, 13.7.2016). A fecha de redacción del presente artículo, la situación sobre la propuesta es la siguiente: el 23 de enero de 2019, el Comité de Representantes Permanentes (Coreper) confirmó su respaldo a las modificaciones propuestas, con vistas a retomar las negociaciones técnicas con el Parlamento Europeo. Actualmente, el Parlamento Europeo parece mantener su apoyo al acuerdo provisional alcanzado en junio de 2018, sin reabrir nuevas negociaciones sobre la cuestión.

que se le conceden, estableciendo normas uniformes. Por su parte, igualmente debía presentarse una propuesta por la que se revisa la Directiva sobre condiciones de acogida, armonizándose en mayor medida en la UE de forma que, aumentando la perspectiva de integración de los solicitantes, se reduzcan los movimientos secundarios. Finalmente, en esta segunda fase la CE, en coherencia con el compromiso de reforzar las vías legales de entrada en Europa, debía proponerse un marco estructurado de Reasentamiento de la Unión.

Lo que no deja de llamar profundamente la atención dado que, salvo la Directiva de protección temporal de 2017, las Directivas de reconocimiento, acogida procedimiento y los Reglamentos de Dublín III y Eurodac habían sido sometidos a evaluación y modificación concluyéndose sus reformas en el año 2013. Sin duda, nos encontramos ante una *nueva era* en el desarrollo del SECA.

La reforma integral del SECA se diseña, en consecuencia, para garantizar, por un lado, la plena convergencia entre los sistemas nacionales de asilo, reforzando la confianza mutua entre los EEMM y conduciendo hacia el buen funcionamiento del sistema de Dublín. Asegurando, por lo demás, que en cualquier lugar donde se encuentren los solicitantes se les trate de manera equitativa y adecuada. Y, por otro lado, proporcionar las herramientas necesarias que permitan la rápida identificación de las personas que se encuentran en clara necesidad de protección internacional frente a las que no lo necesitan.

El volumen de datos personales que se mueve en el acceso, la tramitación, la derivación de los procedimientos, la determinación del EM responsable para conocer del asilo, los diversos procedimientos de reparto de la carga entre los Estados, la reubicación o el reasentamiento da buena cuenta de la necesidad de abordar y sistematizar el tratamiento de los datos personales de las personas que solicitan protección internacional.

No en vano, a raíz de la propuesta de reforma del SECA que anunció la CE, el Supervisor Europeo de Protección de Datos (SEPD) reconoció la necesidad de reforzar la efectividad de la migración y el asilo en la UE. Al mismo tiempo, destacó que estas mejoras debían acompañarse de un incremento de los derechos e intereses legítimos de las personas que podían verse afectadas por el tratamiento de datos personales, en particular las relativas a grupos vulnerables que requieren de protección específica, como los solicitantes de protección internacional y refugiados. En su Dictamen, recomendó las vías principales sobre las que debía actuarse —principalmente del Reglamento de Dublín, Eurodac— o la necesidad de llevar a cabo evaluaciones completas del impacto sobre la protección de datos y la privacidad[23].

Cuán lejanas parecen haber quedado algunas de las recomendaciones tras el profundo, radical y vertiginoso salto normativo y conceptual que se ha operado en

23 Supervisor Europeo de Protección de Datos (SEPD). Resumen ejecutivo del dictamen del Supervisor Europeo de Protección de Datos sobre el primer paquete de reformas del Sistema Europeo Común de Asilo (Reglamentos Eurodac, EASO y Dublín), enero de 2017 (2017/C 9/04).

apenas un año con la aprobación de los Reglamentos (UE) 2019/817 y 2019/818, para la interoperabilidad entre los sistemas de infomación en la UE, que establecen nuevas operaciones de tratamiento de datos destinadas a identificar a las personas de que se trate. Admitiendo, por los demás, su Considerando 40, que ello constituye una injerencia en los derechos fundamentales reconocidos en los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la UE pero, dado que la aplicación eficaz de los sistemas de información de la UE depende de la identificación correcta de las personas afectadas, «tal injerencia está justificada por los mismos objetivos para los que se ha creado cada uno de estos sistemas: la gestión eficaz de las fronteras de la Unión, la seguridad interna de la Unión y la aplicación efectiva de las políticas de la Unión en materia de visados y asilo» (C.40).

III. UNA PRIMERA APROXIMACIÓN AL MARCO JURÍDICO REGULADOR DEL DERECHO A LA PROTECCIÓN DE DATOS DE LOS SOLICITANTES DE PROTECCIÓN INTERNACIONAL

Tratar de sistematizar el régimen jurídico del derecho a la protección de datos en el SECA no constituye una tarea en absoluto sencilla. De hecho, no se cuentan con estudios monográficos sobre el particular ni siquiera tras la *constitucionalización* del derecho a la protección de los datos personales tras el Tratado de Lisboa[24]. Son múltiples las razones, y de diversos ordenes (jurídico, operativo y metodológico, entre otras), las que podrían aducirse para explicar este déficit de atención doctrinal[25]; ya hoy nada justificables, a pesar de la enorme complejidad que reviste un régimen jurídico en continua evolución a la par que la propia evolución tecnológica en un contexto absolutamente cambiante condicionado por una de las mayores crisis de refugiados tras la Segunda Guerra Mundial.

Con carácter previo, debemos tener presente, al menos, dos variables para desbrozar adecuadamente ese marco jurídico que debe aplicarse en el tratamiento de los datos personales con sus límites y garantías:

Una, que en el procesamiento de los datos personales en este ámbito convergen multitud de organismos en distintos estadios y en diversas fases del proceso. Ello exige tener presente las distintas obligaciones que derivan para los distintos actores que participan con diversos roles, de naturaleza muy diferente, así como

24 En expresión de López Aguilar, J.F., *Europa: Parlamento y Derechos. Paisaje tras la Gran Recesión,* Tirant lo Blanch, 2017, p. 179.

25 El derecho a la privacidad y protección de datos ha sido «la disciplina olvidada» por parte de la doctrina, entre otras razones, porque con mucha probabilidad se ha percibido como un derecho accesorio y subsidiario a los verdaderos problemas de efectividad del derecho a la protección internacional. Ello, sin embargo, no ha resultado óbice para que algún autor como Hathaway haya hecho referencia al derecho a la privacidad en el ámbito del asilo (Hathaway, J. et Foster, M., «Serious harm», *The Law of Refugee Status*. Cambridge University Press, 2014, p. 287).

su función y finalidad (agencias, ONG, organismos asistenciales, autoridades y funcionarios públicos, etc.) en un proceso en el que se debe garantizar el derecho a la protección de los datos personales. En segundo término, y en íntima conexión con la anterior, debe tenerse presente la base jurídica competencial en función de la cual deberá aplicarse los diversos principios que rigen la protección de los datos, especialmente tras la aprobación del RGPD. A lo que debe añadirse todo un cambio conceptual en el Derecho de la UE en el que, para garantizar la seguridad en la UE y, por ende, en los EEMM, los retos deben ser abordados de forma colectiva a través de la apuesta de un eficaz intercambio de información que tendrá un fortísimo y particular impacto en el derecho a la protección de los datos personales.

Teniendo presente las anteriores variables, por lo que respecta al SECA, hasta el año 2013, la protección de los datos personales se ha circunscrito a un régimen jurídico separado por el criterio de especialidad.

Recordemos que, previamente a la entrada en vigor el Tratado de Lisboa, la fragmentación, la falta generalizada de supervisión adecuada y de cooperación *intra* institucional evidenciaron la necesidad de replantear el marco jurídico de protección de datos en el ámbito de la protección internacional. La Directiva 95/46/CE de protección de datos en la UE, como es bien conocido, constituyó el eje vertebral del régimen de protección de datos durante las dos últimas décadas. Con la entrada en vigor del Tratado de Lisboa, se produjo el desarrollo más relevante de la protección de datos al ser reconocido explícitamente la protección de las personas físicas en relación con el tratamiento de los datos personales como derecho fundamental —previsto tanto en el art. 8.1 CDFUE como en el art. 16.1 TFUE—. Sin embargo, el ámbito de la protección internacional fue atribuido igualmente al ámbito de la seguridad, circunscrita a la Declaración 21, anexa al acto final de la Conferencia Intergubernamental que se adoptó en el Tratado de Lisboa plasmando así, su naturaleza legislativa específica. La Decisión Marco 2008/977/JAI ha constituido el principal instrumento de excepción a la aplicación de la directiva básica por cuestiones radicadas en seguridad nacional, sin perjuicio de la normativa específica que aproximó, todavía más, las cuestiones de seguridad en el ámbito de la protección de datos[26].

Ahora bien, el derecho a la protección de datos en materia de asilo fue una realidad con la entrada del Programa de Estocolmo, aplicado por el Plan de Acción que se adoptó en junio de 2010, en el que apostó decididamente por

26 En ámbito penal, además de la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, fue aprobada la Decisión 2008/616/JAI del Consejo de 23 de junio de 2008 relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. Por otro lado, la Decisión Marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea. Igualmente, se promulgaron numerosos textos conexos con la protección de datos y el intercambio de información en el sector penal europeo.

fortalecer la seguridad interior y exterior y la cooperación entre autoridades judiciales y con terceros países. En este punto, adquirió cuerpo el tratamiento de datos automatizados de los migrantes como un instrumento más del acceso efectivo y controlado a la UE. De hecho, el Programa subrayó la importancia de garantizar la seguridad de los propios ciudadanos europeos, contar con controles fronterizos reforzados para impedir la inmigración ilegal y la delincuencia transfronteriza al mismo tiempo que se debía garantizar el acceso a las personas en clara necesidad de solicitar protección internacional. Igualmente, instó a que los países de la UE hicieran uso de la justicia en red, es decir, de las tecnologías de la información y la comunicación aplicadas al ámbito de la justicia como método para robustecer la confianza mutua y la coherencia respecto al ordenamiento jurídico internacional a fin de crear un entorno jurídico seguro para interactuar con los países que no pertenecían a ella, previendo la necesidad no solo de reforzar el papel de Frontex sino también la operatividad de las bases de datos sobre migración y asilo (en especial Eurodac, VIS y Schenguen) para responder de manera más eficaz a los múltiples desafíos que presentaba una fragmentada normativa de protección de datos en el ámbito del SECA.

Sin embargo, el trascendental avance del Programa en la protección efectiva de los datos de los solicitantes de asilo y refugiados resultó, a todas luces, insuficiente. La regulación de protección de datos de los solicitantes de asilo no se adecuó de forma expresa al régimen general de la Directiva 95/46/CE de protección de datos, a pesar de su expresa remisión en el actual Reglamento Dublín III. Del mismo modo, y a pesar de las continuas excepciones por razones de seguridad, tampoco ha resultado aplicable, en toda su extensión, el régimen jurídico contemplado en la Decisión Marco 2008/977/JAI[27], sin perjuicio del tratamiento de datos por parte de las instituciones y organismos comunitarios, agencias comunitarias especializadas en seguridad, migración y asilo así como autoridades policiales o agencias de seguridad y espionaje que únicamente se encuentran vinculados por sus propios reglamentos de desarrollo.

Efectivamente, paralelamente al régimen general, ha coexistido normativa especializada que ha venido apartándose de la aplicación uniforme de este marco jurídico, en especial, los distintos sistemas de información y bases de datos (concretamente, Eurodac), el tratamiento de datos por parte de las instituciones y organismos comunitarios así como agencias comunitarias especializadas en

27 En cuyo art.1 se establecía que el fin era garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal (apartado 1.º) y era susceptible de aplicación tanto al tratamiento automatizado como no automatizado, total o parcial (apartado 3.º). Ahora bien, se excluía expresamente de aplicación aquéllas cuestiones que afectaban directamente con los intereses esenciales de seguridad del Estado y con las actividades específicas de inteligencia en el sector de la seguridad del Estado (apartado 4.º), lo que evidencia la exclusión, cuanto menos parcial, del tratamiento de datos en el ámbito de la inmigración y asilo.

seguridad, migración y asilo (Frontex, EASO o Europol), los cuales se encuentran vinculados directa o indirectamente con la gestión y protección de los solicitantes de protección internacional.

La falta de respuestas fue especialmente compensada por los organismos especializados en asilo. El ACNUR viene exigiendo la imperante necesidad de elevar la seguridad jurídica en este ámbito desde el año 2008, en el que reconoció, por primera vez, la necesidad de implementar un sistema reforzado de protección de datos para refugiados en un contexto con fuertes diferencias entre unas organizaciones y otras en la propuesta del anterior Reglamento de Dublín.[28] Fruto de ello, las organizaciones comenzaron a analizar sus procedimientos en relación con el procesamiento de los datos personales. En el año 2010, la Organización Internacional para las Migraciones (OIM) llevó a cabo una reestructuración interna para reforzar la protección de datos en el ámbito de la migración y asilo,[29] procedimiento que se encontró con el escaso interés del Comité Internacional de la Cruz Roja (CICR). En 2013, revisó sus normas profesionales para mejorar los sistemas de gestión de la información confidencial, aunque no llevaron a cabo cambios reales y efectivos.[30] Ello, a pesar de que, tal y como recogían los informes de noviembre de 2013, fueron identificadas brechas de seguridad de considerable entidad en *Red Rose*, un sistema online para gestionar la distribución de ayuda utilizada por el CICR y que lo hacía especialmente vulnerable a los piratas informáticos.[31] Este incidente puso en evidencia las profundadas debilidades en el procesamiento de datos personales, especialmente en un contexto en el que las agencias humanitarias recurren cada vez más a la ayuda de sistemas de procesamiento de datos digitales como técnicas eficientes de asistencia y cooperación. De hecho, el propio CICR establecía en su manual de protección de datos y acción humanitaria que se desencadenaban importantes motivos de interés

28 ACNUR, Comentarios del ACNUR sobre la Propuesta de la Comisión Europea para la reforma del Reglamento del Parlamento Europeo y del Consejo por el que se establecen los criterios y mecanismos para la determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o por un apátrida («Dublín II») (COM(2008) 820, de 3 de diciembre de 2008).

29 Organización Internacional para las Migraciones (OIM), Manual de Protección de Datos, 2010. http://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf.

30 Comité Internacional de la Cruz Roja, *«normativa profesional relativa a la labor de protección llevada a cabo por los agentes humanitarios y los defensores de los derechos humanos en los conflictos armados y otras situaciones de violencia»*, 2013. https://www.icrc.org/spa/assets/files/2011/p0999-spa.pdf.

31 *Mautinoa Technologies* identificó varios problemas de seguridad en una plataforma de software utilizada por las agencias de ayuda para almacenar los datos de las personas vulnerables, exponiéndolos a «riesgos muy significativos». Red Rose lo negó en todo momento. Sin embargo, se constató que el proveedor de sistemas y tecnologías de pago *Mautinoa*, ingresó en un servidor de la ONG en la nube, *Catholic Relief Services*, y accedió a nombres, fotografías, detalles familiares, números PIN y coordenadas del mapa para más de 8,000 familias que recibían asistencia de la ONG en África Occidental. En respuesta, *Oxfam*, uno de los varios clientes de la plataforma, comunicó la suspensión temporal de nuevos datos en los sistemas Red Rose, como medida de precaución. La información puede encontrarse en: https://www.irinnews.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk. Accedido el 18 de abril de 2018.

público en la recopilación de datos personales cuando la actividad en cuestión forma parte de un mandato humanitario establecido en virtud del derecho internacional.[32]

Por lo que respecta al estatuto del ACNUR, prevé la recopilación de información personal sobre una base legítima reformado en resoluciones posteriores de la Asamblea General de la ONU.[33] En mayo de 2015, adoptó su política sobre la protección de los datos personales[34] e implementó por un lado, una evaluación de impacto en la privacidad (PIA) sobre las intervenciones basadas en dinero en efectivo en el año 2015[35] y por otro, la herramienta de proyección demográfica *DPT00L* a finales de 2017. Un potente sistema de información que registraba información de los sujetos que requerían asistencia procesando y compartiendo información personal de forma anonimizada con las distintas operaciones del ACNUR. Este sistema supuso un serio precedente en el incremento de las garantías de protección de datos, privacidad y seguridad de este colectivo a la par que aumentó la eficiencia del procedimiento de protección internacional.[36] Además, una auditoria desarrollada en el Programa Mundial de Alimentos de las Naciones Unidas volvió a detectar ese mismo año serias anomalías en la seguridad en la protección de datos.[37]

32 Comité Internacional de la Cruz Roja (CICR), *Handbook on Data Protection in Humanitarian Action,* Kuner C., Marellica M. (eds.), 2017, parágrafo 3.4, p. 49.

33 Véase ACNUR, Note on the Mandate of the High Commissioner for Refugees and his Office, octubre de 2013, disponible en: http://www.unhcr.org/uk/526a22cb6.pdf

34 Este estudio exige que el personal del ACNUR aplique toda una serie de principios en el procesamiento de datos personales: (a) Procesamiento legítimo y justo, (b) Especificación de la finalidad, (c) Necesidad y proporcionalidad, (d) Precisión, (e) Respeto de los derechos del interesado, (f), Confidencialidad, (g) Seguridad y (h) Responsabilidad y supervisión. ACNUR, *«Política sobre la Protección de Datos Personales de las Personas del Interés del ACNUR»*, mayo 2015. http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=58aadc2b4.

35 Este PIA ha tenido como objetivo la identificación de los riesgos de privacidad que planteaba su programa y buscar mejorar las salvaguardas que pueden mitigar esos riesgos, abordando el desafío de garantizar que los datos de refugiados no fueran utilizados para fines distintos a los especificados inicialmente. ACNUR, *Privacy Impact Assessment of* UNHCR *Cash Based Interventions*, diciembre de 2015. Accesible en: http://www.globalprotectioncluster.org/_assets/files/tools_and_guidance/cash-based-interventions/erc-privacy-impact-assessment-of-unhcr-cbi_en.pdf

36 El sistema, *a priori* garantista con la privacidad y la seguridad de los sujetos, no aporta conclusiones exactas sino que estima el número futuro de personas desplazadas o solicitantes de asilo. Para ello, cruza distintos datos ya recogidos (concretamente, el número de nacimientos, muertes así como la magnitud de la migración forzada o personas desplazadas en un determinado territorio) para predecir, a corto plazo, los posibles movimientos ordinarios. Ahora bien, el sistema únicamente funcionará ante contextos y proyecciones muy concretos puesto que no prevé sucesos extraordinarios que, en buena medida, son las causantes de los desplazamientos de personas a gran escala. Más información acerca del proyecto: http://demographicprojection.unhcr.org/ o http://www.unhcr.org/statistics/unhcrstats/59bbeb384/unhcr-statistics-technical-series.html

37 La citada auditoria exigió la necesidad de definir y clarificar las funciones y responsabilidades de los socios, la implementación efectiva de los compromisos políticos con la seguridad y la privacidad de los datos de los beneficiarios y fortalecer los procesos de gestión de identidad e información de los beneficiarios. Naciones Unidas, Programa de Alimentos Mundial, Internal Audit of Beneficiary Management Office of the Inspector General Internal Audit Report, noviembre de 2017 (AR/17/17). Disponible en: https://docs.wfp.org/api/documents/WFP-0000040084/download/?_ga=2.43869413.1326768420.1516256388-1682848339.1511261484

En consecuencia, el nivel de protección de los datos personales de los solicitantes de protección internacional ha resultado significativamente limitado y difuso. La convergencia y el despliegue de multitud de organismos evidencia la especial dificultad de determinar un régimen jurídico común y coherente. De hecho, fruto de ello, apuntaba Boehm que las prácticas a la hora de procesar, gestionar, compartir y eliminar sus datos personales en el ámbito de la migración y asilo han resultado frecuentemente intrusivas.[38]

En el plano jurisprudencial, debe traerse a colación que la STJUE, de 17 de julio de 2014, *Y.S c. Minister voor Immigratie, Integratie en Asiel Minister voor Immigratie, Integratie en Asiel c M.S.*[39], constituye una de las escasas resoluciones que analiza el impacto de la anterior legislación de protección de datos sobre un solicitante de asilo que solicitó un permiso de residencia temporal. En este caso, el TJUE clarificó el alcance de los datos personales de acuerdo con la Directiva 95/46/CE y proporcionó orientación sobre el procedimiento de acceso a los datos. Específicamente, atribuyó la mera obligación para las autoridades de dar traslado al solicitante de un resumen completo en el que constasen los datos personales de forma inteligible. El TJUE alegó que no era necesario proporcionar tales datos «en la forma material en que existía o se había registrado inicialmente», una interpretación que permitió a las autoridades nacionales un mayor margen de discrecionalidad necesario para proteger sus intereses y, al mismo tiempo, cumplir con el deber de información así como de acceso, rectificación o supresión de los datos.

El TJUE, basándose en las conclusiones del Abogado General, señaló que los solicitantes tenían un interés legítimo en acceder a la información puesto que podía resultar incompleta o haber cambiado, lo que podía condicionar seriamente la decisión futura. Igualmente, clasificó tres tipos de datos: aquellos meramente abstractos, hechos ilustrativos no relacionados con una persona identificable y la clasificación legal de los hechos relacionados con una persona identificada o identificable y su evaluación en el contexto de la ley aplicable; siendo este último la única tipología de datos que entraba dentro del ámbito de aplicación de la Directiva[40].

En definitiva, pese a que constituye un deber garantizar la protección efectiva por parte de aquellos sujetos que recopilan información personal, el amplio despliegue de organismos asistenciales y la incidencia de la seguridad nacional

38 Boehm, F., «Data Protection Standard in the AFSJ», en *Information sharing and data protection in the Area of Freedom, Security and Justice — Towards harmonised data protection principles for information exchange at EU-level*, Springer, 2011, p. 28.

39 Asuntos acumulados C-141/12 y C-372/12.

40 Peers apuntó que, el fallo resultó especialmente útil para los solicitantes de asilo pudieran hacer valer (por diferentes medios) el derecho a una buena administración en contra de las autoridades nacionales Peers, S., «Data protection rights and administrative proceedings», de 17 de julio de 2014. Accesible en: http://eulawanalysis.blogspot.com/2014/07/data-protection-rights-and.html.

exige una profunda revisión del complejo marco jurídico actual y cuyas garantías específicas para el procesamiento de datos personales resultan difusas, incluso tras la aplicación del actual régimen jurídico de protección de datos en Europa, integrado principalmente por el RGPD y la Directiva 2016/680 de protección de datos en el ámbito penal.

Ello obliga a analizar las propuestas de reformas pendientes a la luz del RGPD que derogó la Directiva 95/46/CE. Sin embargo, y como el Reglamento de Dublín remite en materia de protección de datos a la Directiva derogada, conviene detenerse en las disfuncionalidades que las remisiones a la misma genera para abordar las excepciones que, sobre esta materia, regirán en la propuestas pendientes de reforma de los instrumentos del SECA y analizarlos a la luz del RGPD. RGPD que se aplica, no se olvide, al tratamiento de datos personales con fines de interoperabilidad por parte de las autoridades nacionales en virtud de los Reglamentos de interoperabilidad a menos que sean las autoridades designadas o los puntos de acceso centrales de los Estados miembros quienes lleven a cabo dicho tratamiento por razones de prevención, detección o investigación de los delitos de terrorismo u otros delitos graves (C. 53 Reglamentos 2019/817 y 2019/818).

IV. SEGURIDAD Y PROTECCIÓN DE DATOS EN EL VIGENTE REGLAMENTO DE DUBLÍN III Y SU REMISIÓN A LA DEROGADA DIRECTIVA 95/46/CE

El Reglamento de Dublín III ha sido coronado como herramienta jurídica clave para interpretar el resto de la legislación aplicable dentro del ámbito del SECA. El Considerando 26 atribuye a la anterior Directiva 95/46/CE, carácter esencial en la aplicación al tratamiento de datos personales por los EEMM con arreglo a este Reglamento. Del mismo modo, el Considerando 27 prevé que, en el supuesto de intercambio de datos personales en el seno de un traslado (incluidos datos de carácter sensible), debe garantizar una asistencia adecuada por parte de autoridades para también asegurar la continuidad de la protección de los derechos reconocidos, instando a la adopción de disposiciones especiales para garantizar la protección de los datos relativos a los solicitantes que se encuentren en esa situación. Al margen de los mencionados considerandos, el art. 34.9 regula una contundente aplicación de esta Directiva en los supuestos de derecho a la información, especialmente, en caso de trasgresión de este derecho *«por razón, por ejemplo, de su carácter incompleto o inexacto, tendrá derecho a su rectificación o supresión»*. Además, el art. 38 establece las medidas necesarias para garantizar la Seguridad en el ámbito de protección de los datos.

No cabe duda de que el mencionado Reglamento, atendiendo a un criterio de especialidad, ha establecido la facultad de regulación específica en materia de protección de datos aplicable a los solicitantes de protección internacional, previendo exclusivamente la adopción de una Directiva de protección de datos

derogada en la aplicación de las obligaciones activas dirigidas a las autoridades de las instituciones comunitarias así como nacionales, las cuales juegan un papel fundamental en la consecución de los objetivos establecidos en el Reglamento. Sin embargo, coexisten una serie de riesgos de enorme calado que han rebajado los derechos y garantías de los interesados en el ámbito de la protección internacional y que se destacan a continuación:

1. Los responsables de la toma de decisiones se enfrentan a un conflicto que emerge de una escasa formación acerca de cuándo y cómo pueden recopilar, procesar, almacenar, analizar, usar y compartir información personal. La falta de habilidades profesionales evidencian un problema propenso a poner en serio peligro la seguridad de los migrantes y solicitantes de protección internacional.[41] La responsabilidad de proteger o *data responsability* no solamente abarca la seguridad de los EEMM sino también la información y datos personales de lo individuos, elemento clave para garantizar su seguridad personal. Ello exige la ponderación los dos intereses en conflicto y su impacto en el procesamiento de la información personal, un campo emergente que busca ir más allá de las preocupaciones de privacidad hacia cuestiones directamente vinculadas con la seguridad nacional.

Esta situación contraría el mencionado Reglamento, que fue pionero en destacar la necesidad de formación en el ámbito de la protección de datos de las autoridades así como de generar un alto nivel de conocimiento de las autoridades competentes en materia de asilo, haciendo una especial mención a la capacidad y formación óptima para reunir las condiciones necesarias para la prestación de una asistencia adecuada para garantizar la continuidad en la protección de los derechos. El RD III alude en los mencionados considerandos, a un criterio de especialidad en el tratamiento de estos datos para garantizar, entre otros, la protección de los datos personales de los solicitantes de protección internacional (en particular, datos especialmente sensibles como los relacionados con la salud) de conformidad con la Directiva 95/46/CE de protección de datos.

2. Este grupo vulnerable se enfrenta a un potencial acceso por parte de una lista compuesta por un gran conjunto de autoridades nacionales y europeas. Además, se adiciona el acceso y comunicación de este tipo de información por parte de otros organismos y agencias comunitarias e internacionales[42] lo que supone un reto de enorme calado a la hora de procesar, gestionar y comunicar la información y datos de carácter personal.

41 Scarnecchia D.P., Raymond N.A., Greenwood F., Howarth C, Poole D.N., A Rights-based Approach to Information in Humanitarian Assistance. PLOS *Currents Disasters*, ed. 1, 20 de septiembre de 2017, p. 4.

42 Concretamente, la Agencia Europea de la Guardia de Fronteras y Costas (Frontex), la Oficina Europea de Apoyo al Asilo (EASO) u organizaciones internacionales como el Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR).

3. Por lo que respecta al tratamiento de datos personales de solicitantes de protección internacional y refugiados, conviene destacar que la alta sensibilidad de la mayor parte de los datos personales susceptibles de tratamiento —datos frecuentemente biométricos donde también resultan susceptibles de inclusión los motivos de persecución que fundamentarán y sustentarán la solicitud de protección internacional—. El propio procedimiento de protección internacional tiende a recopilar una gran tipología de datos e información personales y que abarca tanto aquellos identificadores entre los que se incluyen nombres, nacionalidades, lugar de procedencia y fecha de nacimiento como los extensos datos de carácter sensible. Sobre estos últimos, desde una vertiente meramente formal, se trata de datos que, por su tipología, son considerados sensibles y que engloban desde las actuales huellas dactilares como las imágenes faciales que prevé la nueva Propuesta de Eurodac. Por lo que respecta a la vertiente material, puede incluirse información pertinente que justifica la persecución que han sufrido los individuos en el país de origen y que motiva, por tanto, el derecho a la protección internacional.

En consecuencia, en el ámbito de la protección internacional emerge un conflicto constitucional de primer orden que viene dado, básicamente, por un vigente RD III que deriva a una derogada Directiva de protección de datos, una generalizada escasa formación de las autoridades nacionales, así como el acceso y procesamiento de datos por parte de autoridades nacionales y europeas que actúan bajo una base legal poco homogénea atendiendo a su finalidad. Una situación con efectos adversos en la protección efectiva de la información de los solicitantes de asilo y que se agrava no solo por la tipología de datos personales —frecuentemente sensibles— sino también en virtud de la persecución que sufre este colectivo por parte de un difuso número de actores tanto en estados de origen, tránsito o incluso mafias organizadas expertas en interceptar a estos colectivos de personas. Además, estos sujetos frecuentemente no disponen de identificación alguna o incluso recurren a identificaciones falsas tras una incesante labor por parte de mafias organizadas en fronteras exteriores de la UE.[43]

Por todo ello cabe concluir apuntando a la dificultad en la obtención de datos personales fehacientes y contrastados para la correcta verificación de las causas que llevan a solicitar protección internacional en la UE ha generado un marco jurídico en el que coexisten generalizadas limitaciones en la efectividad de este derecho.

43 EMN Ad-Hoc Query on Impact of false/forged documents in the immigration and asylum procedures, 16 de junio de 2017. Accesible en: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/2017.1204_lu_impact_of_falseforged_documents.pdf

Para un studio sobre la cuestión, veáse Hollins K. Comparative international approaches to establishing identity in undocumented asylum seekers, Lowy Institute's Migration and Border Policy Project, n.º 8, 11 de abril de 2018. Accesible en: https://www.lowyinstitute.org/publications/comparative-international-approaches-establishing-identity-undocumented-asylum-seekers

V. EL RGPD Y SU IMPACTO EN LAS PROPUESTAS DEL SECA

5.1. **La previsión del RGPD en las propuestas de reglamento de Dublín, Eurodac y Procedimiento**

Una de las primeras cuestiones que merece especial análisis se centra en determinar el complejo régimen aplicable al procesamiento y protección de la información y datos personales concernientes a los migrantes y, en concreto, a los solicitantes de protección internacional. Tanto el RGPD como la Directiva de protección de datos en el ámbito policial y de justicia no resultan fácilmente identificables en lo que respecta a la aplicación a los sujetos de protección internacional.

En primer lugar, conviene precisar que la corrección de errores del RGPD, en la versión de la traducción española, modificó el ámbito de aplicación del art. 3.2 en el tratamiento de datos personales de interesados de aquellos residentes en la UE por aquellos que simplemente se encuentren en la UE.[44] Esta corrección se encuentra plenamente en sintonía con el Considerando 14 RGPD, que establece que la protección otorgada por el mismo debe aplicarse a las personas físicas independientemente de su nacionalidad o de su lugar de residencia.

De hecho, tal y como destacó el Consejo Europeo de Protección de Datos en las Directrices 3/2018,[45] los controladores o procesadores no establecidos en la UE pero que llevan a cabo actividades de procesamiento comprendidas en el art. 3.2 están obligados a designar un representante en la UE y cumplir con el RGPD. Aún así, reconoce que surgen muy diversos escenarios en función del tipo de actividades de procesamiento, la entidad que lleve a cabo estas actividades de procesamiento o la ubicación de dichas entidades. Por lo tanto, apunta a la necesidad de que los controladores y procesadores, especialmente aquellos que ofrecen bienes y servicios a nivel internacional, realicen una cuidadosa evaluación de sus actividades de procesamiento, a fin de determinar si el procesamiento de datos personales queda dentro del alcance del RGPD.

Por lo que respecta al régimen jurídico de la propuesta del SECA, la aplicación del RGPD se extiende a los solicitantes de protección internacional. Por un

44 Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). L 127/3, 23 de mayo de 2018. Este particular ha sido puesto de relieve por parte de un sector doctrinal que lo ha tildado «como poco, de llamativa» (Vid. García Mahamut, R., «Del Reglamento General de Protección de Datos a la LO 3/2018 de protección de datos personales y garantías de los derechos digitales», *El Reglamento General de Protección de Datos un enfoque nacional y comparado. Especial referencia a la lo 3/2018 de protección de datos y garantía de los derechos digitale*s (R. García Mahamut y B. Tomás Mallén (eds.) Tirant lo Blanch, Valencia, 2019, p.107.

45 Consejo Europeo de Protección de Datos, Directrices 3/2018 sobre el alcance territorial del RGPD GDPR (Artículo 3) — Versión para consulta pública. Adoptado el 16 de noviembre de 2018. Disponible en:

lado, tanto en la propuesta de RD IV[46] (Considerando 38) como la propuesta de Reglamento de Procedimiento[47] (Considerando 68), establecen la obligación de que las autoridades de los EEMM apliquen las altas garantías previstas en el RGPD para el procesamiento de datos personales. Como regla general, estas incluirán las altas medidas de seguridad en el tratamiento de los datos personales así como la prevención del acceso a los datos por parte de terceros, la divulgación de información personal ilícita o no autorizada o la alteración o la pérdida de los datos personales procesados de acuerdo con los arts. 38 RD III y 50 PRD IV.

Por otro lado, no son escasas sus referencias en la Propuesta de reglamento de Eurodac. El Preámbulo así como varias disposiciones de la propuesta hacen explícita referencia al RGPD. Entre ellas, se encuentra la prohibición de trasferencia de datos a los terceros países salvo que estos países apliquen las garantías del RGPD o en virtud de lo que establezcan las normas nacionales adoptadas con arreglo a la Directiva de protección de datos en el ámbito penal, en cuyo caso parece facultarse la trasferencia con la finalidad de cooperación entre ambos países (Considerando 50). También prevé los derechos de acceso, rectificación y supresión conforme al capítulo III del RGPD (art. 31.1), la supervisión por parte de las autoridades nacionales de control a que se refiere el art. 46.1 RGPD (art. 32.1) o la trasferencia de datos a terceros países a efectos de retorno (art. 38.1).

Además, el alcance del RGPD ha excedido del propio SECA. El ACNUR posee una guía sobre protección de datos del año 2018 en el que adecua su aplicación en sus prácticas de procesamiento de información.[48] Igualmente, dispone de una plantilla sobre el intercambio de datos entre este con un gobierno nacional[49] con la finalidad de proteger la privacidad y confidencialidad de los datos individuales por defecto y promoviendo, al mismo tiempo, mejoras en la prestación de servicios para los refugiados bajo los principios de necesidad y proporcionalidad. Como regla general, no incluye datos de carácter sensible y su incorporación responde a estrictos criterios de necesidad y limitación de la finalidad. Particularmente relevante resulta no solo las continuas referencias al RGPD así como al Convenio 108+[50] sino toda una serie de excepciones en su

46 Comisión Europea, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida (texto refundido) — COM(2016) 270 final

47 Comisión Europea, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece un procedimiento común en materia de protección internacional en la Unión y se deroga la Directiva 2013/32/UE, COM(2016) 467 final 2016/0224 (COD)

48 ACNUR, Guidance on the Protection of Personal Data of Persons of Concern to UNHCR, 23 de agosto de 2018, p. 15. Disponible en: https://www.refworld.org/docid/5b360f4d4.html

49 ACNUR, Modelo de acuerdo sobre el intercambio de datos personales con los gobiernos en el contexto de la entrega del proceso de determinación de la condición de refugiado, Ginebra: ACNUR. Disponible en: https://www.unhcr.org/50a646f79.pdf

50 Sobre esta interrelación, merece especial lectura: Tomás Mallén S., «Las sinergias entre el reglamento general de protección de datos de la Unión Europea y el Convenio 108+ del Consejo de Europa», *El*

aplicación, precisamente, en virtud del interés superior de estos sujetos como es el caso del consentimiento.[51] Y en todo caso, dispone de un Delegado de Protección de Datos (DPO) que se encarga de revisar todos los acuerdos de transferencia de datos personales a una autoridad nacional policial o judicial y proporcionar asesoramiento, en consulta con las excepciones que se exijan por parte de la Sección de Protección y Seguridad Nacional de la División de Protección Internacional.

No cabe duda de que la previsión del RGPD se encuentra directamente tipificado en la propuesta de reforma del SECA, especialmente en lo relativo a la aplicación de las medidas técnicas y organizativas adecuadas para garantizar que la seguridad de los datos y, concretamente, la prevención del acceso a los datos por parte de terceros, la divulgación de información personal ilícita o no autorizada o incluso la alteración o la pérdida de los datos personales procesados de acuerdo. Situaciones que, en caso de producirse, pondrían en serio peligro la seguridad del solicitante, expuesto a su interceptación y persecución por parte de países de origen o terceros países de residencia. Ahora bien, como veremos a continuación, el RGPD se encuentra excluido de este ámbito, propiciando un régimen jurídico especialmente amplio y difuso que puede rebajar los estándares que prevé la propuesta de reforma del SECA en materia de protección de datos.

5.2. ¿Se excluye la aplicación del RGPD en el ámbito de la protección internacional?

El régimen aplicable de protección de datos en el ámbito del SECA parece que opta por seguir extendiendo un difuso marco jurídico en la protección de los derechos de los solicitantes que se aparta de las garantías del RGPD, previendo

*Reglamento General de Protección de Datos un enfoque nacional y comparado. Especial referencia a la lo 3/2018 de protección de datos y garantía de los derechos digitale*s (R. García Mahamut y B. Tomás Mallén (eds.) Tirant lo Blanch, Valencia, 2019, pp. 59-91.

51 Por ejemplo, como regla general, el procesamiento de datos personales por parte del ACNUR para una solución distinta a la inicial no comunicada previamente al interesado requiere, como regla general, del nuevo consentimiento de acuerdo con el (art. 5 (b) RGPD). Sin embargo, las distintas actuaciones necesarias para paliar las brechas que ponen en serio riesgo la seguridad nacional faculta a que el ACNUR y el resto de organizaciones y agencias puedan apartarse de esta limitación con objeto de llevar a cabo todas las actuaciones necesarias para asegurarla siempre y cuando se lleven a cabo de forma proporcional e individual y ateniendo a «imperantes motivos de interés público» (art. 6.1 (e) RGPD). Y pese a que su mandato no permite proporcionar asistencia a sujetos que pueden comprometer la seguridad de los estados, reconoce que, frecuentemente, lo cierto es que frecuentemente no resulta viable la obtención del consentimiento de todos los sujetos interesados. Asimismo, incorpora la adecuación de múltiples disposiciones del RGPD como la implementación de todas las medidas razonables para garantizar que los datos personales inexactos se eliminen o corrijan sin demora indebida, y no conservándose más tiempo del necesario para los fines para los que fueron recopilados (art. 5.1 (d) RGPD), el fiel respeto a los principios de necesidad, proporcionalidad y limitación de almacenamiento (art. 5.1 (e) RGPD y art. 5.4 (e) del Convenio 108+). Véase sobre el particular: ACNUR, *Guidance on the Protection of Personal Data…*, *op. cit*, 2018, p. 65; FRA y Consejo de Europa, Handbook on European data protection law, Sección 3.5, 2018, p. 129.

una serie de limitaciones con objeto de salvaguardar los intereses nacionales y la seguridad de los EEMM.

Qué duda cabe de que las autoridades nacionales requieren de un marco jurídico más flexible que el previsto en el RGPD para la tramitación de las solicitudes de protección internacional. Sus altas garantías reconocidas pueden limitar seriamente las actuaciones de autoridades nacionales que gestionan solicitudes de asilo lastrando el procedimiento de asilo, el cual exige identificar y discernir las distintas categorías de sujetos así como proporcionar las condiciones de acogida necesarias durante la tramitación de una forma eficiente.

El Considerando 16 RGPD excluye de su aplicación las *«actividades relativas a la seguridad nacional y (…) al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión».* En similares términos, el art. 2(2)(b) RGPD excluye el procesamiento de datos personales por parte de los EEMM cuando realizan actividades relacionadas con el asilo, el control de fronteras y la inmigración.

Y sobre esta exclusión, lo cierto es que algunos países como el Reino Unido o Alemania han restringido los derechos de los migrantes y solicitantes de protección internacional, por ejemplo, el derecho de acceso a información, consentimiento, etc.[52]

Por tanto, se contemplan persistentes limitaciones en el ejercicio de este derecho a menudo necesarias puesto que de lo contrario, podría impedirse o dificultarse *de facto* la investigación que requiere determinar los motivos y existencia de la persecución sufrida. Unas restricciones que se encuentran igualmente previstas en la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas[53] donde el art. 15, en relación con la anterior directiva de protección de datos, las preveía siempre y cuando resultaran necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la

52 En el Reino Unido, la ley de Protección de datos de 2018 contiene una cláusula en materia de protección de datos (*Data Protection Bill Clause*). Concretamente, la Sección 15, exceptúa a la inmigración de la aplicación del RGPD en su parágrafo 4.º. Una cláusula que, de acuerdo con las afirmaciones del Ministerio del Interior del Reino Unido, evitaría que quienes se enfrentan la deportación, pudieran cuestionar la exactitud de sus datos personales así como obtener un amplio acceso a los mismos. Accesible en: https://www.theguardian.com/technology/2018/mar/05/home-office-immigration-data-access-eu-citizens-data-protection-bill. En este mismo sentido, Alemania aprobó la ley destinada a fortalecer la seguridad fronteriza a expensas de la privacidad de los solicitantes de asilo. Un proyecto de ley anunciado por el Ministerio del Interior en Febrero de 2017 permitiría a las autoridades alemanas tomar datos de teléfonos inteligentes, portátiles y demás dispositivos de solicitantes de asilo en el país, con el fin de determinar sus identidades y nacionalidades (anteriormente, los funcionarios solo podían tomar datos personales con el consentimiento de los solicitantes de asilo). La Oficina Federal de Migración y Refugiados (BAMF) estableció que la medida está dirigida a los solicitantes de asilo que llegan a Alemania sin pasaporte o con documentos falsificados, una ley a todas luces desproporcionada con el derechos a la privacidad. Sobre el particular, véase: TANGERMANN J., Documenting and Establishing Identity in the Migration Process Challenges and Practices in the German Context *Focussed study by the German National Contact Point for the European Migration Network (EMN)*. Working Paper n.º 76, 27 de septiembre de 2017.

53 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. OJ *L 201, 31.7.2002, p. 37–47*

seguridad de los estados. Limitaciones a día de hoy necesarias y especialmente aplicables en las técnicas y los procedimientos para la gestión eficiente de las fronteras exteriores, considerado el elemento central del sistema de control de fronteras.

Paralelamente, la intervención directa e indirecta de un amplio conjunto de actores en la gestión de la información y datos personales de los solicitantes de protección internacional ha propiciado la creación de un extenso marco jurídico especializado. Como hemos señalado, Frontex o la futura Agencia de Asilo de la UE se rigen por el Reglamento (UE) 2018/1725 y las autoridades policiales nacionales, Europol o incluso servicios de inteligencia o espionaje nacionales disponen de un elevado margen de actuación, apartándose generalizadamente de las garantías que prevé el mencionado RGPD en virtud de la aplicación de sus propios reglamentos de desarrollo.

Esta amplia flexibilidad de las autoridades policiales en el cumplimiento de la legislación protección de datos ha sido recientemente objeto de debate en la STEDH *Catt c. Reino Unido* de 24 de enero de 2019[54] que limitó las facultades de la policía en relación con la recopilación y retención de los datos personales. Concretamente, el TEDH determinó que Reino Unido había violado el derecho a la privacidad del Sr. Catt, un activista por la paz que, a pesar de no tener antecedentes ni posibilidades de cometer actos de violencia, sus datos se encontraban en una base de datos de carácter extremista. En particular, recordó la importancia de examinar el cumplimiento de los principios del art. 8 CEDH y, especialmente, en contextos donde las facultades otorgadas a los estado resultan confusas, propiciando un elevado riesgo de arbitrariedad en virtud del incesante desarrollo tecnológico de los sistemas de información empleados por las autoridades policiales y agencias de seguridad. Además, el mencionado tribunal destacó el mayor nivel de protección que deben tener los datos que revelan una opinión política, lo que parece ampliarse a cualquier dato de carácter sensible.

Pese a todo, coexiste un régimen jurídico enormemente amplio y divergente que viene a justificarse por la exigencia de una exhaustiva actuación nacional, en cooperación con un amplio espectro de organismos europeos, que determinen —previamente al objeto principal de examinar la solicitud de protección internacional— los siguientes extremos:

1. La identificación de los nacionales de terceros países y examinar si el sujeto puede ser susceptible de impactar negativamente en la seguridad nacional.
2. La determinación del EM responsable para conocer la solicitud de protección internacional de acuerdo con el «Sistema de Dublín».
3. El mantenimiento de la supervisión y el control de los flujos migratorios.
4. La optimización de la capacidad de los sistemas nacionales de asilo mediante una sinergia eficiente de medios materiales, humanos, financieros y de infraestructuras basado en los flujos migratorios concretos,

54 STEDH, *Catt c. Reino Unido*, de 24 de enero de 2019 (Solicitud no. 43514/15).

escenario complejo en los Estados especialmente afectados por la carga desproporcionada de solicitantes de protección internacional.

5.3. **La aplicación de la Directiva 680/2016 de protección de datos en el ámbito penal en el SECA**

Las solicitudes de protección internacional se ha vinculado frecuentemente a escenarios que ponen directamente en riesgo el mantenimiento de la seguridad de los EEMM. Una situación que ha evidenciado la estructural carencia de seguridad jurídica en el tratamiento de la información y datos personales en el ámbito de la gestión de la migración y asilo de la UE. Tanto es así, que el SEPD se hizo eco de las crecientes preocupaciones de la UE en la lucha contra el terrorismo y la necesidad de encontrar un equilibrio entre la seguridad y la privacidad en el procesamiento de datos personales, especialmente, las gestionadas por parte de las autoridades policiales. Reconoció la necesidad de introducir mejoras importantes sobre acciones vulnerables de este colectivo con objeto de evaluar mejor los derechos e intereses legítimos de las personas relevantes que puedan verse afectadas por el tratamiento de datos personales.[55]

Pese a los ingentes esfuerzos de la propuesta de reforma del SECA por aumentar las garantías del derecho a la protección de datos mediante la aplicación del RGPD, todo parece indicar que, fruto de la ponderación entre seguridad europea y protección datos de los solicitantes de asilo, las limitaciones en este derecho se equipararán principalmente a la Directiva 680/2016 de protección de datos en el ámbito penal.

El amplio despliegue de autoridades policiales en la gestión de las solicitudes por las constantes remisiones del asilo a las cuestiones sobre las que penden la seguridad de los EEMM exige un marco jurídico que flexibilice el margen de maniobra de las autoridades nacionales aunque ello implique una limitación en los derechos de los solicitantes de asilo. Sobre este extremo, el art. 3 apartado 2 y 4 de la propuesta de Eurodac equiparan los términos definidos en la Directiva de protección de datos de ámbito penal a los definidos en el presente Reglamento, el art. 36.2 (h) prevé adecuarse al RGPD o Directiva a la hora de crear perfiles que describan las funciones y responsabilidades de las personas autorizadas al acceso, registro, actualización, supresión y búsqueda de datos de Eurodac. Un supuesto de alternancia entre las dos normativas de protección de datos que repite el art. 37.4 a la hora de levantar las prohibiciones de trasferencia de datos. Ahora bien,

55 Supervisor Europeo de Protección de Datos, *Dictamen del Supervisor Europeo de Protección de Datos sobre el segundo paquete de fronteras inteligentes de la UE,* 13 diciembre de 2016 (C 463/11). Véase también Supervisor Europeo de Protección de Datos, *Protección de Datos y Privacidad en 2018: Más allá del RGPD,* 20 Marzo 2018. https://edps.europa.eu/press-publications/press-news/press-releases/2018/data-protection-and-privacy-2018-going-beyond-gdpr_en

la plasmación del RGPD en la propuesta de reforma de Eurodac recibió críticas del ECRE que aconsejaba eliminar estas referencias en las disposiciones en la mencionada propuesta.[56]

En este sentido, en Eurodac, el RGPD podría resultar aplicable a las cuestiones relacionadas con el acceso de la autoridades policiales a Eurodac de modo que, una vez hayan sido extraídos todos los datos personales, el tratamiento de los mismos que efectúen los servicios de seguridad en Eurodac estará sujeto a la nueva Directiva relativa a la protección de datos en el ámbito penal de acuerdo con lo dispuesto en el art. 35 de la mencionada propuesta. El alcance sobre la efectiva aplicación del RGPD debería incluirse en el informe sobre su evaluación y revisión que, de conformidad con el art. 97 RGPD, deberá trasladar la CE al Parlamento Europeo y al Consejo —y que, a más tardar, se llevará a cabo el 25 de mayo de 2020—.

Por lo que respecta a la mencionada Directiva, su aplicación se encuentra en plena sintonía con la Directiva 2017/541 relativa a la lucha contra el terrorismo[57], ambas enmarcadas dentro del *Plan de Acción* presentado por la CE para intensificar la lucha contra la financiación del terrorismo.[58] De hecho, esta última Directiva constituye un buen ejemplo de integración pues incluye una cláusula explícita —la primera de este tipo— sobre derechos fundamentales, y, al mismo tiempo, tiene en cuenta parámetros necesarios en este aspecto como los principios de necesidad y proporcionalidad de las interferencias con los derechos de libertad de circulación, protección de datos y libertad de expresión que reconocen los arts. 8 y 11 CDFUE. No obstante, la seguridad de los ciudadanos de la UE sigue constituyendo una de las prioridades legislativas de la UE tal y como así parece reflejar la Declaración conjunta sobre las prioridades legislativas de la UE para 2018-2019, de 14 de diciembre de 2017.[59]

La vinculación entre ambos instrumentos jurídicos resulta especialmente notoria. La Directiva de protección de datos 680/2016 regula la libre circulación

56 European Council on Refugees and Exiles (ECRE), Comments on the Commission Proposal to recast the Eurodac Regulation COM(2016) 272, Julio de 2016, p. 6.

57 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 sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo.

58 Comisión Europea, Comunicación de la Comisión al Parlamento Europeo y al Consejo, Plan de acción para intensificar la lucha contra la financiación del terrorismo, COM/2016/050 final, 2 de febrero de 2016 (http://europa.eu/rapid/press-release_IP-16-202_es.htm). Además, tal fue el impacto del terrorismo, que la CE en abril 2016, la elaboró las primeras estrategias para allanar el camino hacia una Unión de la Seguridad genuina y efectiva (http://europa.eu/rapid/press-release_IP-16-1445_es.htm) que se extiende hasta nuestros días.

59 Esta Declaración pretende tomar medidas encaminadas a garantizar que las autoridades de los Estados miembros identifiquen los sujetos que cruzan la frontera exterior común de la UE, establecer sistemas de información interoperables en la UE para la gestión de la seguridad, las fronteras y la migración, y a reforzar los instrumentos de lucha contra el terrorismo. Declaración conjunta sobre las prioridades legislativas de la UE para 2018-2019. OJ C 446, 29.12.2017, p. 1–3.

de datos personales entre las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública en el seno de la Unión y la transferencia de estos datos personales a terceros países y organizaciones internacionales, a la par que se garantiza un alto nivel de protección de los datos personales. La Directiva prevé la adopción de normas específicas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, excluyendo el tratamiento de datos personales en el marco las actividades relacionadas con la seguridad nacional.[60] En todo caso, el art. 15 dispone las autoridades nacionales deberán restringir los derechos de los interesados en caso única y exclusivamente de que comprometan seriamente su seguridad.

Además, la Directiva de lucha contra el terrorismo concreta las mencionadas disposiciones no solo ponderando la seguridad y protección de datos bajo el paraguas de criterios de eficacia, necesidad y proporcionalidad sino aludiendo al respeto de las normas de la Unión sobre protección de datos establecidas en la Directiva (UE) 2016/680 en lo que respecta al intercambio de información en la lucha contra el terrorismo. Ello, sin perjuicio de respetar los principios establecidos en el art. 2 TUE, los derechos y libertades fundamentales y los principios consagrados en la CDFUE, en particular, la prohibición de discriminación, el respeto a la vida privada y familiar y a la protección de datos de carácter personal.[61]

Con ello, salvo la tramitación y gestión de la información por parte de autoridades policiales, las correspondientes limitaciones de derechos en la protección de datos en relación con el ámbito de asilo deberán responder a inexorables razones de seguridad nacional que no permitan —en modo alguno— ampliar y equiparar los derechos de acuerdo con las disposiciones del RGPD. Estas restricciones deberán efectuarse individualmente, sobre una solicitud en concreto y que, en todo caso, no deberán causar indefensión al interesado, máxime habida cuenta de la posición vulnerable del solicitante y la importancia que revisten sus datos personales en todo el proceso de determinación del estatuto de refugiado o protección subsidiaria.

No obstante, la aplicación de la Directiva parece justificarse no solo por el amplio despliegue de autoridades policiales en la gestión de este tipo de información sino por la exigencia que reside en la imperante necesidad de investigar no solo la identidad y el perfil del solicitante sino las causas que motivan su persecución. La mayor flexibilidad que requieren las autoridades administrativas y policiales nacionales en sus actuaciones —especialmente en un contexto de grandes flujos migratorios— donde un amplio número de sujetos solicitan protección internacional o donde las formalidades que requiere el RGPD merecen rebajarse para proteger eficientemente a los sujetos de protección internacional. Ello, a

60 Considerandos 7, 11 y 14.
61 Considerandos 21, 25 y 35.

pesar de la nueva PRD IV, que regula referencias expresas a la protección de los datos personales en materia de acceso, rectificación o supresión de los datos (art. 6. 1h)) a todas las categorías de datos personales (art. 6.1 g)).

Ahora bien, la aplicación generalizada de este marco jurídico supondría a todas luces una criminalización de solicitantes con dos desventajosas consecuencias:

Primero, la diferencia de trato entre los ciudadanos de la UE y los solicitantes de protección internacional puede tener potenciales *efectos discriminatorios* por cuanto supone una equiparación de este vulnerable colectivo a otras categorías de sujetos como potenciales delincuentes o terroristas y donde las limitaciones previstas no resultan aplicables a otras categorías de sujetos —por ejemplo, los turistas que llegan a los distintos países de la UE—.

Segundo, estas limitaciones pueden dificultar excesivamente el acceso de los solicitantes al procedimiento e impedir que los solicitantes de protección internacional puedan comprobar la información y los datos personales que constan la solicitud de protección internacional, produciendo serios obstáculos en la efectividad de este derecho.

5.4. **La seguridad y protección de datos en el actual y futuro Sistema de Dublín**

Para finalizar, debemos hacer especial mención a la breve regulación que protege la información personal en el ámbito del SECA. El Capítulo IX regula en el art. 38 RD III (art. 50 PR IV) la seguridad y protección de datos, uno de los aspectos mas relevantes para garantizar la seguridad de los datos relativos a los solicitantes de protección internacional. El mencionado artículo habilita a los EEMM a adoptar todas aquellas medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos personales transmitidos con la finalidad de evitar el acceso o la divulgación ilícitos o no autorizados, la alteración o la pérdida de los datos personales tratados, pues puede suponer un grave peligro para la seguridad e integridad física del solicitante y para la propia viabilidad y credibilidad del sistema en su conjunto. Todo ello deriva en la obligación activa de los EEMM en desarrollar e implementar aquellas medidas oportunas que garanticen el alto más grado de seguridad en la protección de la información.

Por lo tanto, pese a que no puede garantizarse la aplicación del RGPD en las gestión de la solicitudes de protección internacional, esencialmente los derechos a los interesados, el RD III y la PR IV exige adoptar medidas de seguridad elevadas para proteger esos datos.

Este precepto reviste una importancia crucial para proteger eficazmente la información de este grupo especialmente vulnerable por lo que las autoridades de control nacionales deben llevar a cabo un férreo control de la legalidad del tratamiento de datos personales por parte de las autoridades de asilo de los EEMM. Ahora bien, no resulta desdeñable destacar que la nueva Propuesta no alude en el

mencionado art. su adecuación al RGPD sino que prevé directamente tres tipos de autoridades (segundo apartado, art. 50):

Por lo que respecta a las existentes autoridades encargadas del cumplimiento de las obligaciones derivadas del presente Reglamento (art. 35 RD III), el art. 47 PRD IV establece mayores obligaciones de estas autoridades en relación con el mecanismo de asignación. Estas autoridades deben encargarse no sólo de responder a las peticiones de información y toma de cargo sino también a las notificaciones de readmisión y todas aquellas necesarias para dar cumplimiento al mencionado mecanismo.

Además, la PRD IV crea por primera vez dos tipos de autoridades. Por un lado, en virtud de la creación de un sistema automatizado de comunicación entre el sistema central y las infraestructuras nacionales, insta a la creación de autoridades nacionales encargadas de registrar y controlar la cuota de solicitudes de protección internacional y la aplicación del novedoso mecanismo de asignación (art. 44.1 PRD IV). Por otro lado, las autoridades verificadoras para detectar y compartir información de sujetos que pueden suponer una amenaza para la seguridad nacional o el orden público (art. 40 PRD IV). Esta autoridad, dentro del mecanismo de asignación correctora, se corona como una de las novedades que prevé Dublín IV para elevar las garantías contra ataques que comprometen la seguridad nacional.

De hecho, el art. 40 habilita a que el EM beneficiario transmita al de asignación de forma rápida los datos biométricos de los solicitantes justificando a tal fin, la necesidad de evaluar, en el menor plazo posible, si puede catalogarse una amenaza para la seguridad nacional o el orden público. El apartado 2.º ampara compartir toda la información sobre la naturaleza de la alerta con lo servicios de seguridad del EM beneficiario sin necesidad de comunicarse a través de los necesarios canales de comunicación electrónicos del art. 47.4 PRD IV. Una excepción que rebaja la protección de la información transmitida y que deberá, en todo caso, llevarse a cabo de forma individualizada.

Estas novedosas autoridades que prevé la PRD IV ostentan una función instrumental, es decir, pretenden dar efectividad a las nuevas disposiciones que prevé la mencionada propuesta. Pese a que elevan principalmente la seguridad, articulando todo un sistema de detección e intercambio de información entre autoridades nacionales y europeas, lo cierto es que en el caso de que el solicitante pueda ser sospechoso de constituir un peligro para la seguridad nacional u orden publico, se dispone de toda una serie de actuaciones excepcionales para garantizar el buen funcionamiento del Reglamento.

Además, el art. 40 PRD IV regula toda una serie de parámetros en relación con la gestión de la información de sujetos que pueden comprometer la seguridad de los Estado y que distinguen entre:

1. El deber de información entre el EM de asignación y de acogida. El primer párrafo del apartado 2.º art. 40 PRD IV exige al primero informar al

segundo de la existencia de dicha alerta, especificando los servicios de seguridad del de solicitud que hayan sido plenamente informadas.

2. La exigencia de dejar constancia de la existencia de la alerta en el sistema automatizado, con arreglo al art. 23, apartado 2, letra d) PRD IV en un plazo de una semana a contar desde la recepción de las impresiones dactilares de conformidad con el art. 40.2 segundo párrafo PRD IV).
3. El sometimiento al procedimiento acelerado que dispone el apartado 3.º art. 40 PRD IV. En este sentido, cuando el resultado de la verificación de seguridad confirme que, por razones fundadas, puede considerarse al solicitante un peligro para la seguridad nacional o el orden público, el EM beneficiario de solicitud será el EM responsable y examinará la solicitud por el procedimiento acelerado (art. 31, apartado 8, de la Directiva 2013/32/UE).

En relación con la legislación de protección de datos, lo cierto es que la PRD IV únicamente dispone en el Considerando 33 que deben establecerse «*normas apropiadas para aquellos casos en que haya motivos fundados para considerar que un solicitante constituye un peligro para la seguridad nacional o el orden público»,* especialmente, normas relativas al intercambio de información entre las autoridades competentes responsables en materia de asilo de los EEMM.

El principio de limitación de la finalidad resulta el único «tímido límite» en la mencionada propuesta donde el apartado 4.º únicamente dispone el intercambio de esta información para los fines de evaluación de un solicitante y su potencial amenaza con la seguridad nacional u orden publico. Todo ello, sin perjuicio del régimen sancionador del art. 40 del Reglamento Dublín III (art. 50 PRD IV), que deja en manos de los EEMM, la adopción de las medidas necesarias para garantizar que toda utilización indebida de los datos tratados de conformidad con el presente Reglamento sea objeto de una sanción efectiva, proporcionada y disuasoria, incluidas las sanciones administrativas y penales previstas en el Derecho nacional.

VI. REFLEXIONES CONCLUSIVAS

La protección de datos de carácter personal en el SECA constituye un campo emergente que debe afrontar la ponderación entre los incesantes retos que afectan a la seguridad europea con aquellos aspectos relacionados con la privacidad y protección de datos mediante una nueva arquitectura jurídica que afronte no solo los problemas de seguridad y protección internacional, sino que también asegure la protección efectiva de la información y datos personales de este colectivo vulnerable.

El alcance de este derecho y la determinación del *régimen jurídico* resulta especialmente complejo en virtud de su naturaleza específica. Por una parte, el actual RD III prevé la adopción de una Directiva de protección de datos que, a día de hoy, está derogada en virtud de la aplicación del RGPD y de la Directiva

2016/680 de protección de datos en el ámbito penal. Por otra, el despliegue de un amplio conjunto de actores en la gestión de la información y datos personales de los solicitantes de protección internacional ha propiciado la creación de un extenso y difuso marco jurídico. El Reglamento (UE) 2018/1725 resulta de aplicación para los organismos y agencias especializadas en gestión del asilo —como Frontex o la futura Agencia de Asilo de la UE— si bien, también se disponen persistentes exclusiones por parte organismos policiales nacionales y europeos, servicios de inteligencia o espionaje.

Este difuso régimen jurídico de protección de datos en el ámbito del SECA refleja una elevada inseguridad jurídica en la determinación del régimen jurídico de la protección de los datos personales en la actualidad. Si bien, parece solventarse, parcialmente, por las remisiones de la aplicación del RGPD tanto en la Propuesta de Reglamento de Dublín, Eurodac como la de Procedimiento, no es menos cierto que requerirá modificaciones de enorme calado que incluyan, con carácter general, las altas medidas de seguridad en el tratamiento de los datos personales así como la prevención del acceso a los datos por parte de terceros, la divulgación de información personal ilícita o no autorizada o la alteración o la pérdida de los datos personales procesados tal y como dispone el Capítulo IX de la PRD IV en su art. 50. Además, esta previsión se encuentra en directa contradicción con el RGPD, que excluye directamente de aplicación sobre el ámbito del asilo, el control de fronteras y la inmigración y ni que decir tiene, la seguridad nacional. Una incoherencia jurídica que pretende reflejar el espíritu del nuevo SECA, el cual apuesta decididamente por reforzar el derecho a la privacidad y protección de datos y que debería abordar la CE en el informe sobre su evaluación y revisión al Parlamento Europeo y al Consejo antes del 25 de mayo de 2020 tal y como así prevé el art. 97 RGPD.

Pese a ello, actualmente la propuesta de reforma del SECA permanece ajena a cuestiones de gran entidad en relación con la protección de datos. En primer lugar, cabe advertir la escasa formación de las autoridades sobre la legislación de protección de datos hasta el potencial acceso e intercambio de información de autoridades de los EM y de organismos europeos o la interoperabilidad entre los distintos sistemas de información. En segundo lugar, la extensión de la plena aplicación del RGPD podría suponer una excesiva limitación de los EEMM en la consecución de los objetivos encaminados a gestionar eficaz y eficientemente las solicitudes de protección internacional y preservar su seguridad nacional. Un conflicto de intereses que no deberá facultar a que las autoridades nacionales limiten de forma generalizada e indiscriminadamente los derechos de los solicitantes sino que deberán responder a imperantes razones concretas de seguridad nacional en aras de aumentar la seguridad jurídica en un ámbito tan sensible y fragmentado como este. De lo contrario, seguirá persistiendo no solo una criminalización de este colectivo, intolerable en cualquier régimen democrático, sino una falta generalizada de confianza en el procedimiento que puede poner en peligro la viabilidad del SECA en su conjunto.

A nuestro juicio, este ámbito exigirá el continuo equilibrio entre dos factores *a priori* opuestos o contradictorios entre sí, pero que *de facto* no dejan de complementase para la consecución de diversos objetivos. Por un lado, la protección de los solicitantes de protección internacional —que merece el mayor grado de apertura de los Estados, pues deben cumplir con sus obligaciones internacionales para ofrecer protección efectiva— así como ofrecer una respuesta efectiva a facilitar la movilidad y la mejor gestión fronteriza, y por otro lado, la respuesta eficaz que deben proporcionar los Estados en la gestión de la inmigración y la prevención de amenazas contra la delincuencia, crimen organizado o terrorismo.

Debemos seguir insistiendo en la complejidad de un marco normativo que, utilizando expresión del SEPD, está integrado por demasiados «elementos móviles». Ello no permite evaluar el alcance de las implicaciones que en materia de garantía de los derechos de protección internacional y protección de datos arroja una normativa europea absolutamente dispersa que no guarda coherencia en los tiempos de aprobación y negociación de los distintos instrumentos legales y que, por ende, no garantiza seguridad jurídica alguna.

Dicho todo lo anterior, los EEMM deberían elevar en sus legislaciones nacionales determinados derechos de los solicitantes de protección internacional de conformidad con el RGPD, en particular, los derechos de información y acceso a los datos personales —así como el cumplimiento de los principios que rigen en el RGPD— y limitarlos en supuestos concretos que puedan comprometer su seguridad. De este modo, se solventaría la inseguridad jurídica actual en este ámbito marcado por las continuas vinculaciones entre seguridad que parecen restringir el derecho a la protección de datos en el ámbito de la protección internacional.

***

TITLE: *The protection of asylum seeker´s personal data in the (new) European Common Asylum System: major challenges and serious shortcomings*

ABSTRACT: *The present work addresses an innovative legal analysis on the treatment and protection of personal data about asylum and subsidiary protection seekers in the comprehensive reform of the Common European Asylum System (CEAS). This reform, among other countless aspects, has increased the effective EU Information Management as the key to protect external borders, improve the management of migration flows and contribute to the enhancement of internal security. The applicable data protection legislation is significantly fragmented, complex and diffuse since, despite the GDPR excludes from its scope asylum-related activities, border control, and immigration is directly defined in the proposed Dublin IV, Procedures and Eurodac regulations. At the same time, the persistent linkages to the security of Member States can reflect the potential application of the Data Protection Directive on Police Matters. In addition, the interoperability of different information systems, the deployment of specific bodies (such as Frontex or EASO) as well as law enforcement authorities are bound directly by their own regulations. Consequently, this fragmented and particularly complex legal framework constitutes the subject of the study.*

RESUMEN: *El presente trabajo aborda un pionero análisis jurídico sobre la protección y tratamiento de los datos personales de los solicitantes de asilo y protección subsidiaria en la reforma integral en ciernes del*

Sistema Europeo Común de Asilo (SECA). Reforma que, entre otros innumerables aspectos, ha elevado la eficaz gestión de la información de la UE como clave de bóveda para proteger las fronteras exteriores, mejorar la gestión de los flujos migratorios y contribuir a reforzar la seguridad interior.El régimen jurídico en materia de protección de datos resulta especialmente fragmentado, complejo y difuso por cuanto que el RGPD, pese a que excluye de su aplicación las actividades relacionadas con el asilo, el control de fronteras y, la inmigración se encuentra directamente tipificado en las propuestas de Reglamentos de Dublín IV, de Procedimiento y de Eurodac. Paralelamente, las persistentes vinculaciones con la seguridad de los Estados miembros constatan la potencial aplicación la Directiva de protección de datos en el ámbito policial. A ello se le adiciona la interoperabilidad de los distintos sistemas de información, el despliegue de organismos asistenciales en frontera (Frontex o EASO) así como de las autoridades policiales, todos ellos vinculados directamente por sus propios reglamentos de desarrollo. En consecuencia, este marco jurídico fragmentado y especialmente complejo constituye especial objeto de análisis.

KEY WORDS: *international protection, protection and processing of asylum seekers personal data, refugees, subsidiary protection, General Data Protection Regulation, CEAS reform, border security, UNHCR, Dublin IV System, Data Protection Directive in in police matters.*

PALABRAS CLAVE: *protección internacional, protección y tratamiento de datos personales de solicitantes de asilo, refugiados, protección subsidiaria, Reglamento General de Protección de Datos, reforma del SECA, seguridad en fronteras, ACNUR, Sistema de Dublín IV, Directiva de protección de datos en el ámbito policial.*

FECHA RECEPCIÓN: *28.05.2019* FECHA ACEPTACIÓN: *29.07.2019*