Freedom, Security & Justice: European Legal Studies

Rivista quadrimestrale on line
sullo Spazio europeo di libertà, sicurezza e giustizia

2020, n. 1

EDITORIALE SCIENTIFICA
ES

Rivista giuridica on line "Freedom, Security & Justice: European Legal Studies"
www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario

2020, n. 1

PROCESAMIENTO INFORMÁTICO DE DATOS Y PROTECCIÓN DE DERECHOS FUNDAMENTALES EN LAS FRONTERAS EXTERIORES DE LA UNIÓN EUROPEA

Jonatán Cruz Ángeles*

SUMARIO: 1. Introducción. – 2. La política común de gestión del espacio Schengen: un espacio europeo sin fronteras interiores. – 3. La evolución y desarrollo de los *IT Systems* en relación con el control de las fronteras exteriores. – 4. El nuevo sistema integrado de gestión de la información. – 5. Interoperabilidad y protección de derechos fundamentales. – 6. Conclusiones.

1. Introducción

Como es sabido, en el año 2015 llegó a la Unión Europea (UE), a través de la ruta del Mediterráneo oriental, una gran oleada de refugiados que huían de la guerra de Siria. Desde entonces, el número de llegadas irregulares por esta ruta se ha reducido considerablemente, gracias a la estrecha cooperación entre la UE y Turquía[1]. Sin embargo, cuando una ruta de migración parece estar bajo control aparece otra nueva, como es el caso de la ruta del Mediterráneo central, que ha pasado a ser la vía más utilizada para entrar en la UE. Como resultado, en la actualidad, la mayoría de los migrantes, procedentes de países del África subsahariana y de África del Norte, ahora pasan por Libia en su viaje hacia Europa. En este contexto, las instituciones de la UE están tratando de desarrollar una nueva política migratoria, que le permita poder controlar la entrada y salida ordenada de migrantes a través de las fronteras exteriores del espacio Schengen, así como llevar a cabo controles policiales en la lucha contra crímenes graves y/o posibles ataques terroristas.

Si esta nueva política migratoria pretende ser eficaz, es necesario el registro, gestión y tratamiento de los datos personales de todas aquellas personas que entren y/o salgan del espacio Schengen. Por este motivo, la UE ha desarrollado varios sistemas

Double blind peer reviewed article.

* Profesor ayudante doctor en el área de Derecho internacional público y Relaciones internacionales de la Universidad de Jaén. Correo electrónico profesional: jangeles@ujaen.es.

[1] Para un estudio más detallado, *vid.* Infografía – flujos migratorios: rutas del Mediterráneo occidental, central y oriental. Disponible en: https://www.consilium.europa.eu/es/policies/migratory-pressures/

informáticos (con sus correspondientes bases de datos), que facilitan toda una serie de complejos procesos relacionados con la migración, tales como: el registro de entrada y/o salida de todos los migrantes que cruzan las fronteras, el registro y tramitación de una solicitud de asilo, el proceso de solicitud de un visado, la tramitación de una devolución/expulsión de un inmigrante en situación irregular y/o el establecimiento de una orden de prohibición de entrada. Hasta hace poco, estos sistemas estaban fragmentados, estrictamente separados y desconectados. Sin embargo, con el fin de responder mejor a los desafíos anteriormente mencionados, la UE aprobó el pasado 20 de mayo de 2019, los Reglamentos (UE) 2019/817 y 2019/818, que establecen un marco jurídico para asegurar la interoperabilidad de todos estos sistemas operativos, que a partir de ahora intercambiarán información entre sí en tiempo real, lo que ayudará a facilitar la correcta identificación de las personas que cruzan las fronteras y contribuirá a luchar contra posibles usurpaciones de identidad.

Este artículo se plantea con un claro esquema de trabajo. En primer lugar, se presenta al lector una síntesis acerca de la creación y desarrollo de la política común de gestión del espacio Schengen, que le será de utilidad para comprender todo el contexto que condiciona el desarrollo de la política migratoria actual de la UE. A continuación, se analizan cuáles son los principales sistemas informáticos utilizados en los controles fronterizos hasta la fecha – sus objetivos, propósitos, puntos fuertes y posibles puntos débiles –. Todo ello, con la finalidad de plantear en qué consiste el nuevo sistema integrado de gestión de la información en las fronteras exteriores de la Unión Europea, así como qué posibles retos y oportunidades plantea su implementación, en relación con la protección de los derechos fundamentales de todos aquellos viajeros/migrantes que crucen nuestras fronteras.

2. La política común de gestión del espacio Schengen: un espacio europeo sin fronteras interiores

El primer paso hacia la creación de una política común de gestión de las fronteras exteriores se dio el 14 de junio de 1985, cuando cinco de los entonces diez Estados miembros de la Comunidad Económica Europea (CEE) firmaron un tratado internacional, el llamado Acuerdo de Schengen[2], que se complementó, cinco años más tarde, con el Convenio de aplicación del Acuerdo de Schengen[3]. El espacio Schengen, la zona sin fronteras creada por el acervo de Schengen (como se conoce al conjunto de acuerdos y normativa en la materia), comprende actualmente 26 países europeos[4]. La

[2] Acuerdo de Schengen: Acuerdo entre los Gobiernos de los Estados de la Unión Económica del Benelux, la República Federal de Alemania y la República Francesa sobre la supresión gradual de los controles en sus fronteras comunes.
[3] Convenio de aplicación del Acuerdo de Schengen.
[4] En estos momentos, los Estados Schengen son, además de España, Alemania, Austria, Bélgica, Dinamarca, Eslovenia, Estonia, Finlandia, Francia, Grecia, Hungría, Islandia, Italia, Letonia,

normativa que compone el acervo actual de fronteras exteriores de Schengen, que se basa en el acervo original incorporado al ordenamiento jurídico de la Unión Europea por el Tratado de Ámsterdam, se encuentra, actualmente, integrado en una amplia gama de medidas, que pueden dividirse, principalmente, en cinco grandes ramas o áreas de estudio: el código de fronteras Schengen[5] (1); el sistema de información Schengen (2); el fondo de seguridad interior: fronteras y visados (3); el sistema de entrada/salida (4); y Frontex: la agencia europea de la guardia de fronteras y costas (5).

El Código de fronteras Schengen[6], es el pilar central de la gestión de fronteras exteriores, en el que se establece, principalmente, la normativa en materia de cruces fronterizos exteriores, así como la ausencia de controles fronterizos en las fronteras interiores, y las condiciones que regirían una posible reincorporación temporal de los controles fronterizos internos. En el espacio Schengen, con el fin de mantener la seguridad internacional, se ha desarrollado el sistema de información Schengen (SIS), el sistema de gestión de la información más utilizado y eficiente que la Unión Europea ha desarrollado en el Espacio de Libertad, Seguridad y Justicia (ELSJ)[7]. Las autoridades de toda la Unión Europea utilizan el SIS para introducir o consultar alertas para personas y/u objetos. Este sistema contiene más de 80 millones de alertas y ha sido consultado más de 5 mil millones de veces por las autoridades en 2017, desencadenando más de 240.000 alertas[8]. El SIS ha sido reforzado, recientemente, a través de la actualización de normativa que trata de abordar posibles lagunas en el sistema e introduce varios cambios esenciales con respecto a los tipos de alertas introducidas. Tras la reforma de 2018, el alcance del SIS se define en tres ámbitos: cooperación policial y judicial en materia penal[9]; controles fronterizos[10]; y devolución de nacionales de terceros países en

Liechtenstein, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, República Checa, República Eslovaca, Suecia y Suiza.

[5] Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016R0399.

[6] *Ibídem.*

[7] Para un estudio más detallado, *vid.:* A. DI STASI, *Il perfezionamento dello spazio europeo di libertà, sicurezza e giustizia: avanzamenti e criticità*, en ID. (ed.), *Tutela dei diritti fondamentali e Spazio europeo di giustizia,* Nápoles, 2019, pp. 103-147; V.L. GUTIERREZ CASTILLO, M. LOPEZ JARA, *El desarrollo y consolidación del Espacio de Libertad, Seguridad y Justicia de la Unión Europea*, Madrid, 2016, *passim.*

[8] Para más información acerca del sistema SIS/II, *vid.:* https://www.europarl.europa.eu/news/es/headlines/security/20181011STO15882/mejoras-en-el-sistema-de-informacion-de-schengen-infografia.

[9] Reglamento (UE) 2018/1862, del Parlamento y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n. 1986/2006 del Parlamento europeo y del Consejo y la Decisión 2010/261/UE de la Comisión.

[10] Reglamento (UE) 2018/1861, del Parlamento y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n. 1987/2006.

situación ilegal[11]. Estos tres reglamentos han introducido categorías adicionales de alertas al sistema, tales como la alerta sobre sospechosos o personas con una orden emitida de búsqueda y captura, alertas preventivas para casos de niños que podrían sufrir secuestro por parte de sus propios progenitores, alertas con el propósito de devolución a terceros países, además de contemplar una base de datos con huellas dactilares, imágenes faciales y ADN de personas desaparecidas con el fin de confirmar su identidad.

Como es sabido, no todos los Estados miembros tienen fronteras exteriores y, por tanto, no todos los Estados miembros están afectados, en la misma medida, por los flujos de tráfico fronterizo. Por este motivo, la Unión Europea se encarga de intentar compensar parte de los costes para los Estados miembros cuyos límites territoriales actúan como fronteras exteriores de la UE. Para el ejercicio 2014-2020, a través de este mecanismo de reparto de la carga, se han movilizado un total de 3.800 millones de euros[12]. En este contexto, el objetivo principal del fondo de seguridad interior (FSI) es el de contribuir a garantizar un alto nivel de seguridad en la Unión, facilitando al mismo tiempo los cruces de frontera autorizados. Los beneficiarios de los programas implementados en el marco de este fondo pueden ser autoridades locales, organizaciones no gubernamentales (ONGs), organizaciones humanitarias, empresas de derecho público y privado, y organizaciones de educación e investigación.

El control de las entradas y salidas de nacionales de terceros países, que cruzan las fronteras exteriores de los Estados miembros del espacio Schengen, se gestiona gracias al denominado sistema de entradas y salidas (SES)[13]. Se trata de un sistema de información que acelera y refuerza los controles fronterizos para los nacionales de terceros países que viajan a la Unión Europea. Este sistema sustituye el estampado (manual) de los pasaportes en la frontera por el registro electrónico en la base de datos. Adoptado en noviembre de 2017, los principales objetivos del sistema de entrada/salida son: reducir los retrasos en el control fronterizo y mejorar la calidad de los controles fronterizos calculando automáticamente la estancia autorizada de cada viajero (1); asegurar una identificación sistemática y fiable (2); y fortalecer la seguridad interna y la lucha contra el terrorismo permitiendo a las autoridades policiales el acceso a los registros de historial de viajes (3). El acceso al sistema de entrada y salida se concede a las autoridades policiales nacionales y a Europol, pero no a las autoridades de asilo. Se

[11] Reglamento (UE) 2018/1860, del Parlamento y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular.

[12] Para más información acerca del apoyo financiero para las fronteras exteriores de la Unión Europea y la política común de visados: Fondo de Seguridad Interior (FSI), *vid.* Reglamento (UE) n. 515/2014, por el que se establece, como parte del fondo de Seguridad Interior, el instrumento de apoyo financiero a las fronteras exteriores y los visados.

[13] Reglamento (UE) 2017/2226, del Parlamento europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entrada/Salida para registrar datos de entrada y salida y denegación de entrada de nacionales de terceros países que cruzan las fronteras exteriores de los estados miembros y la determinación de las condiciones de acceso con fines policiales, y la modificación del Convenio de aplicación del Acuerdo y los Reglamentos (CE) n. 767/2008 y (UE) n. 1077/2011 de Schengen.

permite la posibilidad de transferir datos con fines de aplicación de la ley y/o de retorno a terceros países y a los Estados miembros de la Unión Europea que no participen en el sistema de entrada y salida, pero en determinadas condiciones. El sistema de entrada y salida registra los datos de los viajeros (nombre, documento de viaje, huellas dactilares, imagen visual y la fecha y el lugar de entrada y salida) al cruzar las fronteras exteriores del espacio Schengen. Las autoridades consulares y fronterizas utilizan este sistema, que se aplica a todos los nacionales de terceros países, tanto a los que requieren un visado como a los que están exentos.

Asimismo, las autoridades fronterizas de los distintos Estados miembros cuentan con el apoyo de la Agencia Europea de la Guardia de Fronteras y Costas (también conocida como Frontex[14]). Esta agencia de la Unión Europea tiene tres objetivos estratégicos: reducir la vulnerabilidad de las fronteras exteriores sobre la base de una conciencia situacional integral (1); garantizar el buen funcionamiento y la seguridad en las fronteras (2) y planificar y mantener la actividad de la Guardia Europea de Fronteras y Costas (3). La agencia Frontex se encarga de monitorear lo que está sucediendo en las fronteras exteriores, donde se puede necesitar su apoyo y, si ésta detecta una posible incidencia en el funcionamiento del sistema de gestión de fronteras de un Estado miembro, como resultado de una evaluación obligatoria de su vulnerabilidad, la Agencia Europea de la Guardia de Fronteras y Costas podrá: exigir que se adopten las medidas correctivas oportunas (1); y/o en caso de que se detecte una incidencia que pueda poner en peligro el funcionamiento del espacio Schengen, podrá intervenir (2) – incluso cuando el Estado miembro, en cuestión, no haya solicitado la intervención, o no la considere necesaria –. Actualmente, Frontex está reclutando y capacitando a más de 700 miembros del cuerpo permanente de la Guardia Europea de Fronteras y Costas, que serán desplegados en distintas operaciones en 2021. Se prevé que, de aquí a varios años, Frontex cuente con 100.000 oficiales de la Guardia Fronteriza y Costera para ayudar a los países europeos con el control de fronteras y gestión de la migración[15].

3. La evolución y desarrollo de los *IT Systems* en relación con el control de las fronteras exteriores

El desarrollo de los distintos sistemas de gestión de la información en las fronteras de Schengen se ha acelerado con la pérdida de vidas a gran escala en el Mediterráneo en los últimos años, junto con la enorme afluencia de refugiados y migrantes desde septiembre de 2015[16]. Antes del estallido de la crisis humanitaria europea de refugiados,

[14] La Agencia Europea de la Guardia de Fronteras y Costas (Frontex) se rige por el Reglamento (UE) 2019/1986, del Parlamento europeo y del Consejo, de 13 de noviembre de 2019, sobre la Guardia Europea de Fronteras y Costas y por el que se derogan los Reglamentos (UE) nº. 1052/2013 y (UE) 2016/1624.

[15] Para más información, *vid.*: https://frontex.europa.eu/about-frontex/foreword/.

[16] E. SCHINDEL, *Blowing off the boat. The sea border crossing to Europe, a navigation on the nature/culture divide*, in *Mobile Culture Studies*, 2015, n. 1, pp. 199-216; ID., *Bare Life at the European*

sólo tres países habían recurrido a la construcción de vallas en las fronteras exteriores para evitar que los migrantes y refugiados llegaran a sus territorios: España (donde se completaron los trabajos de construcción en 2005 y se prorrogaron en 2009), Grecia (finalizados en 2012) y Bulgaria (en respuesta a Grecia, completados en 2014). Contrariamente al artículo 14, apartado 2, del Código de fronteras Schengen, que establece que "la entrada sólo podrá denegarse mediante una decisión fundamentada que indique los motivos precisos de la denegación"[17], un número cada vez mayor de Estados miembros se ha embarcado gradualmente en la construcción de muros fronterizos o vallas con el objetivo de impedir indiscriminadamente que los migrantes y solicitantes de asilo accedan a sus territorios nacionales. Además, sin normas explícitas de la Unión Europea sobre la construcción de vallas en las fronteras exteriores de Schengen, los Estados miembros también han puesto barreras con terceros países (en particular Marruecos y Rusia), incluidos los candidatos de pre-adhesión (la República de Macedonia del Norte, Serbia y Turquía) y Croacia, un país candidato a Schengen de la Unión Europea. También se han construido vallas dentro del espacio Schengen, como la valla entre Austria y Eslovenia, mientras que las prácticas españolas en Melilla han sido objeto de control por parte del Tribunal Europeo de Derechos Humanos de Estrasburgo[18].

En este contexto, la Unión Europea ha hecho un gran esfuerzo por desarrollar distintos sistemas informáticos centralizados a gran escala, tales como: el SIS II (1)[19]; el VIS (2)[20]; el Eurodac (3)[21]; el Sistema de Entradas y Salidas – EES o SES (4)[22]; y el

---

Borders. Entanglements of Technology, Society and Nature, in *Journal of borderlands Studies*, 2016, n. 2, pp. 219-234; ID., *Migrantes y refugiados en las fronteras de Europa. Cualificación por el sufrimiento, nuda vida y agencias paradójicas*, in *Revista de Estudios Sociales*, 2017, n. 35, pp. 16-29.

[17] Código de fronteras Schengen, art. 14.2. La entrada sólo puede denegarse mediante una decisión fundamentada que indique los motivos precisos de denegación. La decisión será tomada por una autoridad facultada por la legislación nacional. Surtirá efecto de inmediato. La decisión justificada que indique los motivos precisos de la denegación se dará por medio de un formulario estándar, tal como se establece en el anexo V, Parte B, rellenado por la autoridad facultada por la legislación nacional para rechazar la entrada. El formulario estándar completado se entregará al nacional de un tercer país en cuestión, quien acusará recibo de la decisión de rechazar la entrada mediante dicho formulario.

[18] Caso *N.D. & N.T. c. España*, n. 8675/15 y 8697/15, de 3 de octubre de 2017; Gran Cámara, Caso *N.D. & N.T. c. España*, n. 8675/15 y 8697/15, de 20 de febrero de 2020.

[19] El Sistema de Información de Schengen de segunda generación (SIS II). Síntesis de los documentos: Reglamento (CE) n. 1987/2006 relativo al establecimiento, funcionamiento y utilización del sistema de información de Schengen de segunda generación (SIS II). Decisión 2007/533/JAI relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II).

[20] El Sistema de Información de Visados (VIS). Reglamento (CE) n. 767/2008 del Parlamento europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los estados miembros (Reglamento VIS).

[21] Reglamento (UE) n. 603/2013 del Parlamento europeo y del Consejo, de 26 de junio de 2013, sobre el establecimiento de "Eurodac" para la comparación de huellas dactilares para la aplicación efectiva del Reglamento (UE) n. 604/2013 que establece los criterios y mecanismos para determinar el Estado miembro responsable de examinar una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o una persona apátrida y sobre las solicitudes de comparación con los datos de Eurodac por las autoridades policiales de los estados miembros y Europol para la ley fines de aplicación y modificación del Reglamento (UE) n. 1077/2011 por el que se crea una

Sistema Europeo de Información y Autorización de Viaje – SEIAV o ETIAS (5)[23] para recopilar, procesar y compartir información vital para la cooperación en materia de seguridad y para la gestión de las fronteras exteriores y la migración. El primero de éstos, el Sistema de Información Schengen (y la segunda generación del sistema) constituye, tal y como hemos visto en apartados anteriores, la base de la cooperación de Schengen. Se trata de un sistema de información que permite que las autoridades nacionales encargadas de realizar los controles pertinentes, tanto en la frontera exterior de Schengen como dentro del espacio Schengen, hagan circular alertas sobre personas buscadas o desaparecidas y objetos como documentos y vehículos robados. El SIS II ofrece información sobre personas que no están autorizadas a entrar o permanecer en el espacio Schengen, o sobre personas en busca y captura por actividades delictivas. El SIS II también contiene información sobre personas desaparecidas, especialmente niños u otras personas vulnerables que necesitan protección. En el SIS II también se recoge información de ciertos bienes, como coches, armas de fuego, embarcaciones o documentos de identidad, que se hayan extraviado, hayan sido robados o se hayan empleado para cometer un delito. En esencia, una autoridad aduanera, policial, judicial o administrativa de un país puede generar una "alerta" donde se describa la persona o el objeto que se está buscando. Se puede generar una alerta por las razones siguientes: para evitar la entrada de personas que no están autorizadas a entrar o a permanecer en el territorio Schengen (1); para buscar y detener a una persona contra la que se ha dictado una orden de detención europea (2); para ayudar a localizar personas, previa petición de las autoridades policiales o judiciales (3); para buscar y proteger a una persona desaparecida (4); y/o para buscar propiedades robadas o perdidas (5). La información almacenada en el SIS II constituye los datos necesarios para identificar a una persona (incluida su fotografía y huellas dactilares) y la información de alerta (incluidas las medidas que se deberán adoptar). El acceso al SIS II está limitado a las autoridades policiales, judiciales y administrativas nacionales. Estas autoridades sólo podrán acceder a los datos que sean estrictamente necesarios para el cumplimiento de su misión. Asimismo, las agencias europeas EUROPOL y EUROJUST gozan de derechos de acceso limitados para realizar determinados tipos de consultas.

Otro sistema de gestión de la información esencial en el Espacio Schengen, es el Sistema de Información de Visados (VIS), que permite a los guardas fronterizos verificar si la persona que presenta un visado es su titular legítimo (o no), con los siguientes objetivos: ayuda a combatir y prevenir posibles comportamientos fraudulentos, como la compra/venta de visados (1); protege a los viajeros de posibles robos de identidad (2); ayuda a determinar qué Estado de la Unión Europea es el

---

Agencia Europea para la gestión operativa de sistemas informáticos a gran escala en el espacio de libertad, seguridad y justicia.

[22] Reglamento (UE) 2017/2226, cit.

[23] El Reglamento (UE) 2018/1240 del Parlamento europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (ETIAS) y se modifican los Reglamentos (UE) n. 1077/2011, (UE) n. 515/2014, (UE) n. 2016/399, (UE) n. 2016/399, (UE) n. 2016/624 y (UE) n. 2017/2226.

responsable de examinar una solicitud de asilo y examinar dichas solicitudes (3); y ayuda a prevenir, detectar e investigar delitos terroristas y otros delitos graves (4). Para ello, una base de datos central segura almacena una serie de datos biométricos del solicitante del visado[24] (diez huellas dactilares y una fotografía digital), junto con los datos proporcionados en el formulario adjunto. No se registran escaneos de dedos para niños menores de doce años ni para personas que físicamente no pueden proporcionar escaneos de dedos. Los viajeros frecuentes al Área Schengen no tienen que hacer nuevos escaneos de dedos cada vez que solicitan un nuevo visado. Una vez que los escaneos digitales se almacenan en VIS, se pueden utilizar para otras solicitudes de visados durante un período de cinco años. En las fronteras exteriores del Área Schengen, los escaneos de dedos del titular del visado se pueden comparar con los que se encuentran en la base de datos. Un desajuste no significa que la entrada se rechace automáticamente, simplemente conducirá a más controles sobre la identidad del viajero.

En esta misma línea de trabajo, contamos también con la base de datos de huellas dactilares de solicitantes de asilo en la Unión Europea (Eurodac)[25], cuya función principal es la de implementar el Reglamento de Dublín[26], en el que se establece que, en principio, el país encargado de examinar la solicitud de asilo será el primer país de entrada. Este sistema común de asilo almacena: diez huellas dactilares (1), el Estado que envía los datos (2); el lugar y fecha de la solicitud de protección internacional (3); y el género del solicitante y el número de referencia asignado (4). Esto permite a las autoridades determinar si los solicitantes de asilo ya han solicitado asilo en otro Estado miembro de la Unión Europea y/o si han transitado ilegalmente por otro Estado miembro de la Unión Europea. El sistema Eurodac permite comparar las huellas digitales del solicitante en los Estados miembros de la Unión Europea y en cuatro Estados asociados de Dublín (Islandia, Noruega, Liechtenstein y Suiza). En el año 2018, el sistema Eurodac analizó un total de 580.845 solicitudes de asilo[27].

En cuanto a la entrada y salida de los nacionales de terceros países que viajan a la Unión Europea, el Reglamento sobre el Sistema de Entradas y Salidas (EES), propone un sistema que registre el momento y lugar de su entrada y salida. Este sistema calcula la extensión de la estancia de corta duración autorizada de manera electrónica,

[24] En relación con las cuestiones socio-políticas y éticas vinculadas con el uso de datos biométricos, *vid.:* J. LODGE, *Developing Biometrics in the EU*. Departamento de Políticas, Parlamento Europeo, Bruselas, 2010, *passim.*

[25] I. VAN DER PLOEG, *The illegal body: Eurodac and the politics of biometric identification*, in *Ethics and Infromation Technology*, 1999, n. 1, pp. 295-302; ID., *Genetics, biometrics and the informatization of the body*, in *Ann Ist Super Sanita*, 2007, n. 1, pp. 44-50; ID., *The body as data in the age of information*, en K. Ball, K. Lyon, D. Lyon (eds.), *Routledge Handbook of Surveillance studies*, Nueva York, Routledge, 2012, pp. 176-183.

[26] El Reglamento de Dublín, oficialmente Reglamento (UE) n. 604/2013, también conocido como Reglamento Dublín III, establece los criterios y mecanismos para determinar el Estado miembro de la Unión Europea responsable del examen de una solicitud de protección internacional - estatuto de refugiado o de protección subsidiaria - presentada por un ciudadano de un tercer país o apátrida.

[27] Para más información, *vid. Asylum quarterly report* (2019-2020), publicado por Eurostat. Disponible en: https://ec.europa.eu/eurostat/statistics-explained/pdfscache/13562.pdf.

sustituyendo al sistema manual[28], emitiendo una alerta a las autoridades nacionales cuando no exista una anotación de salida en el momento de expiración. De esta forma, el sistema también sirve para abordar el problema de las personas que superan la duración autorizada de sus visados de corta duración. Para reducir el tiempo de cruce de la frontera para los nacionales de terceros países y la carga de trabajo para los guardas fronterizos, la propuesta del Sistema de Entradas y Salidas ofrece a los Estados miembros la posibilidad de automatizar la mayoría de los pasos de captura de datos e información, así como las verificaciones de datos. Al utilizar los denominados *quioscos de autoservicio,* los viajeros pueden verificar si sus datos están registrados en el Sistema, tomarse una foto (o, alternativamente, revisar su huella digital) y deben responder a una serie de preguntas. Una vez que el documento de viaje se escanea en los quioscos de autoservicio, se activan todas las verificaciones obligatorias frente a las bases de datos de seguridad. A continuación, el viajero es guiado a un carril de control fronterizo donde, mientras tanto, el guardia de fronteras recibe las respuestas de las bases de datos de seguridad, la confirmación de la identidad del viajero, la duración restante de la estancia y el guardia de fronteras puede hacer más preguntas antes de decidir autorizar (o rechazar) el acceso al espacio Schengen. Este Sistema de Entradas y Salidas está planteado para ser utilizado por las mismas autoridades que utilizan VIS (oficinas consulares y guardia de fronteras). El Reglamento de Entradas y Salidas ofrece la posibilidad de que dichas autoridades accedan a VIS (y viceversa), reduciendo posibles duplicidades en el procesamiento de datos personales. En cuanto a los datos registrados, en principio, el EES sólo almacena la imagen facial de los titulares de los visados (ya que las huellas digitales ya están registradas en VIS). Para los viajeros que carecen de visado, el sistema utiliza una combinación de cuatro huellas dactilares y la imagen facial como identificadores biométricos. Esta elección de identificadores biométricos permite una identificación precisa de los viajeros y reduce los datos registrados en el sistema, al mismo tiempo que asegura una mayor agilidad en los controles fronterizos. Los datos almacenados en EES están protegidos contra posibles de riesgos de abuso, ya que el acceso al Sistema de Entrada/Salida está restringido a autoridades competentes designadas. La transferencia de datos a terceros, ya sean entidades privadas o públicas, está prohibida y todo el procesamiento de datos lo realiza la Agencia de la Unión Europea para la Gestión Operación de Sistemas (eu-LISA) o los propios Estados miembros. Además, existen garantías y mecanismos diseñados para garantizar la protección efectiva de los derechos de los datos personales de los viajeros. Los viajeros tendrán derecho de acceso, rectificación y eliminación de sus datos personales y la protección de la información contenida en el Sistema de Entrada/Salida

[28] La práctica de los sellos estampados en el documento de viaje es laboriosa, no proporciona datos fiables sobre los pasos fronterizos, no permite detectar el rebasamiento de la estancia autorizada de una forma fiable y no puede hacer frente de manera eficaz a lo casos de extravío o destrucción de los documentos de viaje. Además, dichos sistemas no permiten a los Estados miembros de la Unión Europea hacer frente a la creciente presión de los viajeros que entran y salen de la Unión Europea, cuyo número, sólo en las fronteras aéreas, se espera que aumente un 80% de 400 millones en 2009 a 720 millones en 2030.

estará garantizada tanto por el supervisor europeo de protección de datos, como por las autoridades nacionales de supervisión.

Y en último lugar, en relación con los nacionales de terceros países que no requieren visado para entrar en el espacio Schengen, contamos con el proyecto del Sistema Europeo de Información y Autorización de Viaje – también conocido por sus siglas como SEIAV o ETIAS[29] –. Esta base de datos se plantea con el fin de llevar a cabo controles por adelantado sobre los viajeros exentos de visado y denegarles la autorización de viaje si se considera que suponen un posible riesgo para la seguridad de la Unión Europea. La arquitectura de esta base de datos es similar a los sistemas ya existentes que están en vigor, por ejemplo, en los EE.UU. (ESTA), Canadá (eTA) y Australia (ETA/eVisitor), entre otros[30]. La implementación y uso de este Sistema de Información y Autorización de Viajes conlleva varios beneficios, tales como: la mejora de la seguridad interna (1); una mejor prevención de la inmigración ilegal (2); la reducción de los riesgos para la salud pública (3); y la reducción de los retrasos en las fronteras (4). Aunque el sistema lleve a cabo controles previos, la decisión final sobre si concederla o rechazarla, incluso en los casos en que la persona tenga una autorización de autorización válida de viaje, será tomada por los guardias fronterizos nacionales que lleven a cabo los controles fronterizos, de conformidad con el Código de fronteras Schengen. El desarrollo de dicho sistema se encuentra a cargo de la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos a Gran Escala en el Espacio de Libertad, Seguridad y Justicia (eu-LISA)[31]. El Sistema Europeo de Información y Autorización de Viajes cumplirá tres funciones principales: verificar la información presentada en línea por los nacionales de terceros países de terceros países exentos de visado antes de su viaje a la UE (1); tramitación de solicitudes verificándolas con otros sistemas de información de la UE (como el SIS, el VIS, la base de datos de Europol, la base de datos de Interpol, el SES y Eurodac) (2); Emisión de autorizaciones de viaje en los casos en que no se identifiquen elementos que requieran un análisis posterior (3). En junio de 2017, el Consejo decidió dividir la propuesta en dos actos jurídicos distintos[32], debido a que la base jurídica de la propuesta (Schengen) no puede abarcar las modificaciones del Reglamento Europol. El 12 de septiembre de 2019, los

[29] Para más información acerca del COM (2016) 731: Propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establece un sistema europeo de información y autorización de viajes (ETIAS) y se modifican los Reglamentos (UE) n. 515/2014, (UE) n. 2016/399, (UE) n. 2016/794 y (UE) 2016/1624.

[30] W. WALTERS, *Rezoning the global: technological zones, technological work and the (un-)making of biometrics borders*, en V. SQUIRE (ed.), *The Contested politics of Mobility. Border zones and Irregularity*, Nueva York, Routledge, 2011, pp. 51-73.

[31] (Eu-LISA) Agencia Europea para la Gestión Operativa de Sistemas informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia. La Agencia eu-LISA comenzó sus actividades en diciembre de 2012. Se encarga de la gestión operativa de SIS II, VIS y Eurodac. Para más información, *vid.*: https://europa.eu/european-union/about-eu/agencies/eu-lisa_es.

[32] Reglamento (UE) 2018/1240, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y se modifican los Reglamentos (UE) nº. 1077/2011, (UE) n. 515/2014, (UE) n. 2016/399, (UE) n. 2016/1624 y (UE) n. 2017/2226, (UE) n. 2017/2226, (UE), y Reglamento (UE) 2018/1241, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 para establecer un Sistema europeo de Información y autorización de Viajes (SEIAV).

reglamentos que establecen el sistema europeo de información y autorización de viajes fueron firmados por los presidentes de ambas instituciones. Sin embargo, el sistema europeo de información y autorización de viajes no se prevé que esté operativo hasta el próximo año 2021.

4. El nuevo sistema integrado de gestión de la información

La Unión Europea está tratando de mejorar sus sistemas de información con el fin de mejorar la efectividad y la eficiencia de los controles en las fronteras exteriores (1); contribuir a la prevención de la inmigración ilegal y la lucha contra ella (2); contribuir a un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión Europea, lo que incluye el mantenimiento de la seguridad pública y el orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros (3); mejorar la aplicación de la política común de visados (4); ayudar a examinar las solicitudes de protección internacional (5); contribuir a la prevención, detección e investigación de los delitos de terrorismo o de otros delitos penales graves (6); y ayudar a identificar a las personas desconocidas que no puedan identificarse o a los restos humanos sin identificar en caso de catástrofes naturales, accidentes o atentados terroristas (7)[33]. En esta línea de trabajo, se plantea la posibilidad de establecer un marco jurídico para garantizar la interoperabilidad[34] del Sistema de Información de Schengen (SIS), el Sistema de Información de Visados (VIS), Eurodac, el Sistema de Entradas y Salidas (SES), el Sistema Europeo de Información y Autorización de Viajes (ETIAS - SEIAV), y el Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN)[35]. Pero, no se trata de una tarea sencilla, pues dicho marco normativo se enfrenta a una serie de retos, tales como: garantizar la identificación correcta de las personas (1); contribuir a luchar contra la usurpación de identidad (2); mejorar la calidad de los datos y armonizar los requisitos de calidad de los datos almacenados en los sistemas de información de la Unión Europea, respetando al mismo tiempo los requisitos de tratamiento de datos de los instrumentos jurídicos que rigen los diferentes sistemas y las normas y principios en materia de protección de datos (3); facilitar y apoyar la aplicación técnica y operativa por parte de los Estados miembros de

[33] K. TOMASZYCKI, *The interoperability of European information systems for border and migration management and for ensuring security*, en *FACTA UNIVERSITATIS. Series: Law and Politics*, 2018, n. 3, pp. 195-211.

[34] La interoperabilidad se refiere a la capacidad de los sistemas de tecnología de la información y a los procesos necesarios para intercambiar datos y permitir el intercambio de información y conocimientos, con el fin de evitar lagunas de información causadas por la complejidad y fragmentación de estos sistemas.

[35] Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN). ECRIS fue creado en 2012 con el fin de permitir un intercambio eficiente entre los Estados miembros de información relativa a condenas penales impuestas en la UE. Por el momento, la mayor parte de la información que se intercambia se refiere a ciudadanos de la UE. El sistema funciona de forma descentralizada y cada Estado miembro almacena información relativa a sus nacionales.

los sistemas información de la Unión Europea (4); reforzar, simplificar y uniformizar las condiciones de seguridad de los datos y de protección de datos que rigen en los respectivos sistemas de información de la Unión Europea, sin perjuicio de la protección y las salvaguardias especiales otorgadas a ciertas categorías de datos (5); racionalizar las condiciones de acceso de las autoridades designadas al SES, al VIS, al SEIAV y a Eurodac, garantizando al mismo tiempo las condiciones necesarias y proporcionadas para dicho acceso (6); y apoyar los objetivos del SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN (7).

Teniendo en cuenta todo lo anteriormente expuesto, la Unión Europea ha aprobado, recientemente, dos iniciativas legislativas en la materia: el Reglamento por el que se establece un marco de interoperabilidad entre los sistemas de información de la UE sobre fronteras y visados (1)[36] y otro Reglamento por el que se establece un marco para la interoperabilidad entre los sistemas de información de la UE sobre la cooperación policial y judicial, el asilo y la migración (2)[37]. Ambos Reglamentos contemplan la creación de un Portal Europeo de Búsqueda (PEB) con el fin de facilitar el acceso rápido, ininterrumpido, eficiente, sistemático y controlado de las autoridades de los Estados miembros y de las agencias de la Unión Europea a los sistemas de información, los datos de Europol y las bases de datos de Interpol para el desempeño de sus tareas y de conformidad con sus derechos de acceso, así como con los objetivos y fines del SES, el VIS, el ETIAS – SEIAV, Eurodac, el SIS y el ECRIS-TCN. Este portal europeo de búsqueda está compuesto por una infraestructura central, incluido un portal de búsqueda que permite la consulta simultánea (1); un canal de comunicación seguro entre el portal, los Estados miembros y las agencias de la Unión que tengan derecho a utilizar esta herramienta (2); y una infraestructura de comunicación segura entre el portal de búsqueda y los distintos sistemas de gestión de la información (3). El uso de este portal de búsqueda se reserva, única y exclusivamente, a las autoridades de los Estados miembros y a las agencias de la Unión europea que tengan acceso como mínimo a uno de los sistemas de información de la UE, de conformidad con los instrumentos jurídicos que rijan estos sistemas. Asimismo, a los efectos de habilitar el uso del portal de búsqueda, eu-LISA creará, en colaboración con los Estados miembros, una serie de perfiles, basándose en la categoría de los usuarios del portal de búsqueda y en el objeto de sus consultas. Además, el sistema conservará un registro de todas y cada una de las consultas efectuadas, que incluirá: el Estado miembro o la agencia de la Unión que inicia la consulta y el perfil de usuario del PEB utilizado (1); la fecha y hora de la

[36] Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n. 767/2008, (UE) n. 2016/399, (UE) n. 2017/2226, (UE) n. 2018/1240, (UE) n. 2018/1726 y (UE) n. 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo.

[37] Reglamento (UE) 2019/818 del Parlamento y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la Unión Europea 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.

consulta (2); y los sistemas de información de la UE y las bases de datos de Interpol consultados (3).

El nuevo Portal Europeo de Búsqueda permite acceder a un servicio de correspondencia biométrica compartido (SCB compartido), que se compone de una infraestructura central – que sustituirá a los sistemas centrales de los sistemas de gestión de información existentes – y una infraestructura de comunicación segura entre el SCB compartido, el SIS central y un registro común de datos de identidad (RCD). El SCB compartido almacena las plantillas biométricas, creadas como resultado de los datos almacenados en los sistemas de gestión de la información ya existentes[38]. Con este objetivo, el servicio de correspondencia biométrica se encargará de obtener fotografías e imágenes faciales y datos dactiloscópicos del Sistema de Entradas y Salidas (SES), del Sistema de Información de Visados (VIS), y del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular. Esta base de datos biométricos se complementa con un registro común de datos de identidad (RCDI), que creará un expediente individual para cada persona registrada en los sistemas de gestión de la información ya existentes, que contendrá la siguiente información: su nombre completo, sexo, fecha de nacimiento, nacionalidad, tipo y número de documento de viaje y su fecha de expiración. Dicha información se extrae del Sistema de Entradas y Salidas (SES), del Sistema de Información de Visados (VIS) y del Sistema Europeo de Información y Autorización de Viajes (SEIAV). La consulta del RCDI se efectuará por una autoridad policial, cuando no sea capaz de identificar a una persona debido a la falta de un documento de viaje o de otro documento fiable que demuestre su identidad (1); cuando existan dudas sobre los datos de identidad facilitados (2); o cuando la persona no pueda o se niegue a cooperar (3). Dicha consulta no está permitida en el caso de menores de doces años, salvo en supuestos motivados por el interés superior del menor. Asimismo, las autoridades designadas y Europol podrán consultar el RCDI cuando existan motivos razonables para creer que la consulta de los sistemas de información de la UE contribuirá a la prevención, detección o investigación de los delitos de terrorismo u otros delitos graves.

Además, el nuevo sistema integrado de gestión también cuenta con un Detector de Identidades Múltiples (DIM) con el doble objetivo de facilitar los controles de identidad y combatir la usurpación de identidad. Este detector de identidades múltiples se compone de una infraestructura central, que almacena vínculos y referencias a los sistemas de información de la UE y una infraestructura de comunicación segura que conecta este sistema con el Sistema de Información Schengen y las infraestructuras

[38] Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) nº. 767/2008, (UE) 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. Artículo 13. Almacenamiento de plantillas biométricas en el servicio de correspondencia biométrica compartido. 1. El SCB compartido almacenará las plantillas biométricas, que obtendrá de los siguientes datos biométricos: a) los datos a que se refieren el artículo 16.

centrales del Portal Europeo de Búsqueda (PEB) y el Registro Común de Datos de Identidad (RCDI). El detector de identidades múltiples contempla un código de colores, asociados a distintas alertas: el vínculo amarillo (1), identifica un conflicto entre datos de identidad, datos biométricos y/o datos de documentos de viaje, registrados en los distintos sistemas de información (pendiente de comprobación manual por parte de las autoridades competentes); el vínculo verde (2), se muestra cuando las autoridades competentes han comprobado que los datos vinculados por el sistema no constituyen el uso de identidades múltiples por parte del viajero/s afectado/s; el vínculo rojo (3), evidencia que las autoridades competentes han comprobado que, tras la vinculación por parte del sistema de datos de identidad, datos biométricos y datos de documentos de viaje, hay indicios de que una o varias personas están utilizando identidades múltiples. No obstante, la mera existencia de un vínculo rojo no tendrá consecuencias jurídicas para la persona afectada. Y en último lugar, el vínculo blanco (4), es señal de que no hay ninguna incidencia derivada de la vinculación de datos de identidad, datos biométricos y/o datos de documentos de viaje.

En cuanto a posibles responsabilidades derivadas del tratamiento de los datos, se contempla que cualquier persona que sufra un perjuicio, como resultado de una operación ilegal de tratamiento de sus datos personales, por parte de las autoridades habilitadas para acceder al sistema, tendrá derecho a que éstas le indemnicen[39]. Asimismo, se contempla que, tras la entrada en funcionamiento de cada componente de interoperabilidad, eu-LISA se hace responsable de la gestión técnica de la infraestructura central de los componentes de interoperabilidad, incluidos su mantenimiento y los avances tecnológicos. Mientras que, los Estados miembros serán responsables de la integración de sus respectivos sistemas e infraestructuras, así como de la gestión y condiciones de acceso de las autoridades nacionales.

[39] E. HOFFBERGER-PIPPAN, *The Interoperability of EU Information Systems and Fundamental rights concerns*, en *Spanish Yearbook of International Law*, 2019, pp. 426-450.

5. Interoperabilidad y protección de derechos fundamentales

Las soluciones de interoperabilidad deben desarrollarse y diseñarse teniendo en cuenta una serie de derechos fundamentales: proporcionar información de una manera comprensible y transparente (1); respetar la dignidad humana al tomar huellas dactilares (2); tener en cuenta los cuidados y atenciones especiales que requieren los niños al registrar sus datos (3); optimizar el uso de los sistemas de información para rastrear a niños desaparecidos (4); garantizar que se cuente con expertos en derechos fundamentales durante el desarrollo de nuevos sistemas informáticos (5); implementación de fuertes medidas de seguridad para evitar el acceso ilegal a los datos (6); garantizar el derecho a solicitar asilo (7); prohibir la transferencia de datos a terceros países (8); evaluar cuidadosamente cómo el acceso de las fuerzas del orden a los datos puede afectar a los derechos fundamentales de los usuarios (9); desarrollar protocolos de detención que respeten los derechos fundamentales (10): mejorar la calidad de los datos registrados (11); y garantizar el derecho de acceso, corrección y supresión de datos personales (12).

El artículo 5, apartado 1, del Reglamento General de Protección de datos (RGPD)[40] exige que los nacionales de terceros países sean informados acerca de cómo se procesan sus datos de forma transparente, inteligible y fácilmente comprensible. A este respecto, uno de los estudios de la Agencia de Derechos Fundamentales de la Unión Europea (2018)[41] señala el riesgo de que las autoridades, encargadas del control de las fronteras,

[40] 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). Artículo 5. Principios relativos al tratamiento. 1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado (licitud, lealtad y transparencia); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines: de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales (limitación de finalidad); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan (exactitud); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante periodos no más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado (limitación de plazo de conservación); f) tratados de manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (integridad y confidencialidad). 2. El responsable del tratamiento será responsable del cumplimiento de los dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva).

[41] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, U*nder watchful eyes: biometrics, EU IT systems and fundamental rights*, 2018, pp. 29-42.

recopilen datos personales de solicitantes de asilo y visados, así como de los migrantes en situación irregular, y los almacenen, posteriormente, en sistemas de gestión de información, suscitándose la duda acerca de si los usuarios están realmente informados (o no) al respecto. En estos casos, se denuncia que los titulares de derechos, a menudo, no están plenamente informados de todos los aspectos relativos al procesamiento de sus datos y/o tienen dificultad para entender la información que reciben. Además, con la implementación del sistema integrado, basado en la interoperabilidad de los sistemas de gestión de la información tradicionales, se plantea si esta labor podría ser incluso más complicada.

La transparencia sobre el propósito de la toma de huellas dactilares alienta a las personas interesadas a cooperar con las autoridades, evitando así situaciones tensas[42]. No obstante, esta tarea puede resultar complicada para las autoridades, que deben proporcionar información detallada, que abarque todos los aspectos del tratamiento de los datos de los solicitantes de asilo, tal y como exige el artículo 29 del Reglamento Eurodac[43], incluyendo el uso de los datos para la implementación del Reglamento Dublín y para las investigaciones de delitos graves y/o de terrorismo. Los desafíos aumentan cuando se recogen huellas dactilares en situaciones estresantes. Si las autoridades proporcionan información limitada, los solicitantes de asilo y los inmigrantes irregulares perciben que los Estados miembros de la Unión Europea actúan de forma poco transparente, tal y como señalan los estudios (2018) de la Agencia de Derechos Fundamentales de la Unión Europea[44]. Esta falta de información afectará a su voluntad de cooperar con las autoridades de control de fronteras. Por este motivo, la Comisión europea lleva a cabo evaluaciones periódicas de los Estados miembros para determinar si se aplica correctamente el acervo de Schengen. Estas "evaluaciones de Schengen" también abarcan los sistemas informáticos de gestión de la información y son importantes para garantizar el cumplimiento del deber de información, tal y como se incluye en los instrumentos jurídicos que regulan todos los sistemas informáticos, aunque puedan aplicarse restricciones a determinados datos registrados en el SIS II[45].

Asimismo, los datos biométricos deben recopilarse de forma que respeten la dignidad humana. La dignidad humana es inviolable, tal y como lo establece el artículo 1 de la Carta de Derechos Fundamentales de la Unión Europea[46]. Las personas pueden ser físicamente incapaces – debido a discapacidades físicas – o no estar dispuestas a

[42] Para un studio más detallado acerca del registro de datos en Eurodac, *vid.,* C. BAULOZ, M. INELI-CIGER, *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System*, Brill, 2015, *passim.*

[43] Para un estudio más detallado de los derechos de los derechos del sujeto de los datos, *vid.* Artículo 29, Reglamento (UE) n. 603/2013, cit.

[44] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Under watchful eyes*, cit., pp. 43-58.

[45] Para más información acerca de posibles restricciones del deber de informar sobre el propósito del registro de datos en el sistema SIS II, *vid*. Reglamento (CE) n. 1987/2006, cit., y Decisión 2007/533/JAI relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II).

[46] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 1. Dignidad humana. La dignidad humana es inviolable. Será respetada y protegida.

proporcionar sus huellas dactilares. Aunque es poco frecuente, los solicitantes de asilo y los inmigrantes en situación irregular pueden negarse a facilitar el registro de sus datos en Eurodac – un fenómeno que parece no ocurrir en el contexto de VIS. Estas personas pueden mostrarse reacias a facilitar el registro de sus huellas dactilares por varios motivos. Puede deberse a que quieren evitar ser trasladados, en el marco del procedimiento de Dublín, a un Estado miembro de la Unión Europea en el que no quieren permanecer. Sin embargo, la investigación de campo de la Agencia Europea de Derechos Fundamentales (2018)[47] ha revelado que, en algunos casos, los usuarios se niegan a que su biometría sea registrada por miedo a que se compartan sus datos con su país de origen. La voluntad de proporcionar las huellas dactilares aumentaría si los solicitantes de asilo y los migrantes en situación irregular se sintiesen tratados de una forma justa y tuviesen confianza en los procedimientos, y si se les permitiese la reunificación familiar en aplicación del procedimiento Dublín[48]. Según los estudios de la Agencia Europea de Derechos Fundamentales (2018)[49] se han registrado casos en los que se ha detenido y/o utilizado la fuerza para tomar las huellas dactilares a solicitantes de asilo y migrantes en situación irregular. E incluso, se han registrado casos en los que se sospecha que los solicitantes de asilo o inmigrantes irregulares han podido llegar a mutilarse/lesionarse, a propósito, con la finalidad de evitar el registro de sus datos. Las huellas dactilares, a menudo, se registran en situaciones estresantes, por la noche o siguiendo a un gran número de llegadas, por ejemplo. En estas situaciones, aumenta el riesgo de posibles comportamientos policiales inapropiados debido al agotamiento o al estrés. Esto, a su vez, puede socavar la dignidad de la persona a la que se le toman las huellas dactilares. Sin embargo, según la investigación de campo de la Agencia Europea de Derechos Fundamentales (2018)[50], las investigaciones tienden a centrarse en aspectos técnicos de la toma de huellas dactilares, y menos en el tratamiento de los usuarios.

Los sistemas de gestión de la información en frontera afectan a los derechos de los niños de diferentes formas. El artículo 24 de la Carta de Derechos Fundamentales[51] hace hincapié en que el interés superior del menor debe ser una consideración primordial en

[47] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Under watchful eyes: biometrics*, cit., p. 45.

[48] Reglamento (UE) n. 604/2013, cit. (17) Todo Estado miembro debe poder abstenerse de aplicar los criterios de responsabilidad, en particular por motivos humanitarios y compasivos, con el fin de permitir la reunificación de miembros de familia, parientes o cualesquiera otros familiares, y examinar una solicitud de protección internacional presentada en cualquier Estado miembro, aunque dicho examen no sea su responsabilidad según los criterios vinculantes establecidos en el presente Reglamento.

[49] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Under watchful eyes: biometrics*, cit., pp. 49-58.

[50] *Ibídem.*

[51] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 24. Derechos del niño. 1. Los niños tienen derecho a la protección y a los cuidados necesarios para su bienestar. Podrán expresar su opinión libremente. Ésta será tenida en cuenta para los asuntos que les afecten, en función de su edad y madurez. 2. En todos los actos relativos a los niños llevados a cabo por autoridades públicas o instituciones privadas, el interés superior del niño constituirá una ponderación primordial. 3. Todo niño tiene derecho a mantener de forma periódica relaciones personales y contactos directos con su padre y con su madre, salvo si ello es contrario a sus intereses.

todas las acciones que las autoridades públicas ejecuten con respecto a los niños. Esto también se aplica a la toma de huellas dactilares. Las investigaciones de campo muestran esfuerzos limitados para informar a los niños de una forma apropiada, de acuerdo con su edad y madurez, aunque se ha constatado que la policía y los guardas fronterizos, a menudo, dedican tiempo adicional, durante la toma de huellas dactilares, para adaptarse a las necesidades del niño. La investigación de la Agencia Europea de Derechos Fundamentales (2018)[52] también señala incidentes relacionados con el uso de la fuerza para tomar huellas dactilares a menores. El riesgo de estigmatizarlos (en una situación que *per se* ya es traumatizante) es evidente en tales casos. Asimismo, debe tenerse en consideración que, a medida que el niño crece, la precisión de la identificación biométrica disminuye. En estos casos, el riesgo de que los datos biométricos no sirvan para identificar al menor aumenta cuando las huellas dactilares o las imágenes faciales se conservan durante más de cinco años.

Muchos menores no acompañados (MENAs) o separados de sus familias desaparecen tras entrar en la Unión Europea. Algunos de estos niños desaparecidos podrían ser objeto de abuso o explotación, incluida la trata de seres humanos[53]. Los sistemas de gestión de la información podrían servir para mejorar las medidas de protección. Este hecho pone de manifiesto que las políticas en materia de procesamiento de datos en fronteras requieren de un enfoque más centrado en posibles víctimas de delitos[54]. En este contexto, se plantea que los niños pueden querer evitar ser registrados o desaparecer por varias razones. Éstas incluirían la falta de confianza en la reagrupación familiar en el marco del Reglamento Dublín (1), miedo a que se les impida llegar a sus destinos previstos (2); y largos tiempos de tramitación de sus solicitudes de asilo (3). La implementación de la interoperabilidad podría favorecer el rastro de los niños desaparecidos y/o secuestrados, siempre que los Estados miembros de la Unión Europea se encarguen de emitir una alerta en el SIS II cada vez que un MENA desaparezca y se favorezcan las colaboraciones entre las autoridades encargadas de la protección de los menores y las distintas fuerzas y cuerpos de seguridad.

El estado de desarrollo de la tecnología determina las opciones que la Unión Europea y que sus Estados miembros tienen a la hora de crear nuevos informáticos, o las opciones que tienen de mejorar los ya existentes. La industria y la comunidad

[52] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Under watchful eyes: biometrics*, cit., pp. 107-118.

[53] Para un estudio más detallado sobre menores migrantes no acompañados, *vid.,* C. PEREZ GONZALEZ, *Migraciones irregulares y derecho internacional: gestión de los flujos migratorios, devolución de extranjeros en situación administrativa irregular y derecho internacional de los derechos humanos*, editorial tirant lo Blanch, 2012, pp. 137-196.

[54] Opinión n. 8 (FRA). Para apoyar la detección de niños desaparecidos o víctimas de la trata de seres humanos, los Estados miembros de la Unión Europea deben registrar sistemáticamente a los niños desaparecidos en el SIS II. Esto requiere mecanismos de notificación entre los centros de recepción y la policía. Para garantizar que los datos almacenados se utilicen con fines de protección infantil, y no sólo para la aplicación de la ley, los Estados miembros de la Unión Europea deben establecer mecanismos de cooperación eficaces entre las autoridades policiales y de protección de la infancia, así como tutores. Esto debe complementarse con formación/capacitación para aquellos profesionales que puedan encontrarse/tratar con niños en situación de riesgo.

científica pueden desempeñar un papel muy importante en el desarrollo de soluciones técnicas que promuevan el respeto de los derechos fundamentales, incluida la protección de los datos personales. Éstos deben seguir incorporando la protección de datos por diseño y por defecto a los nuevos sistemas de gestión de la información en nuestras fronteras. En este contexto, el principio de limitación de finalidad, tal y como se refleja en el artículo 8.2 de la Carta de Derechos Fundamentales[55], así como en el artículo 5.1 b) del Reglamento General de Protección de Datos (RGPD)[56] y en el artículo 4.1 de la Directiva de tratamiento de datos personales por parte de autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales[57]: exige que los datos personales se procesen únicamente para propósitos específicos, que deben definirse explícitamente. Al optimizar el uso de los sistemas informáticos para combatir la inmigración irregular, así como los delitos graves y/o el terrorismo, existe el riesgo de que los datos puedan utilizarse para fines que no estaban previstos inicialmente. Este riesgo es particularmente alto en el caso de la interoperabilidad de los sistemas informáticos. El artículo 28 y el artículo 32 del RGPD exigen que las instituciones de la UE y los Estados miembros tomen las medidas necesarias para evitar que los datos sean comunicados o puedan acceder a ellos personas u órganos no autorizados. Si los sistemas informáticos se hacen interoperables, los datos personales almacenados en un solo sistema se utilizarán en todos los sistemas para la correcta identificación de una persona. En tales escenarios, garantizar la limitación de propósitos es particularmente difícil. Los sistemas informáticos que incluyen datos sobre solicitantes de asilo pueden ser particularmente atractivos para la piratería informática o para terceros Estados. Por este motivo, deben diseñarse fuertes medidas de seguridad para limitar posibles riesgos de acceso a los sistemas de gestión de la información[58].

[55] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 8. Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

[56] Reglamento (UE) 2016/679, cit. Artículo 5. Principios relativos al tratamiento.

[57] 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.

[58] Opinión n. 10 (FRA). Las instituciones de la Unión Europea y los Estados miembros deben establecer todos los mecanismos razonables para garantizar que los datos almacenados en los sistemas informáticos en el ámbito del asilo y la migración no sean accesibles de forma ilegal. En aquellos casos en los que agentes privados utilicen los sistemas informáticos, deben aplicarse cortafuegos eficaces que les impidan ver datos sin autorización. Las instituciones de la Unión Europea y los Estados miembros deben supervisar el acceso a los sistemas informáticos a través de los archivos de registro. Los archivos de registro deben especificar quién accedió a un determinado sistema y con qué propósito. Las autoridades nacionales de protección de datos y el supervisor europeo de protección de datos deben tener acceso para registrar archivos a petición. Las autoridades sólo deben imprimir y almacenar copias impresas de los datos cuando lo hagan de forma debidamente justificada, y se adhieran a las normas de control de acceso

Los resultados de la investigación de la Agencia Europea de Derechos Fundamentales (2018)[59] revelan que algunos solicitantes de asilo, con las yemas de los dedos lesionadas, no estaban tratando de evitar, de forma intencionada, el registro de sus huellas dactilares. La sospecha de que una persona desee engañar a las autoridades afecta a su derecho de asilo, protegido por el artículo 18 de la Carta de Derechos Fundamentales[60]. La incapacidad física para proporcionar huellas dactilares debido a posibles lesiones en las yemas de los dedos o debido a una incapacidad no debe dar lugar a un trato discriminatorio, prohibido por los artículos 20 (igualdad ante la ley)[61] y 21 (no discriminación)[62] de la Carta de Derechos Fundamentales. En este contexto, debemos tener en cuenta que muchas personas tratan de ocultar su identidad cuando huyen de su país de origen para protegerse. Otros pueden ser físicamente incapaces de obtener los documentos necesarios para entrar de forma legal en el espacio Schengen, tales como un pasaporte y/o un visado, al tratar de escapar de un conflicto armado o de una persecución. En estos casos, Interpol utiliza dos bases de datos: una para documentos de viaje robados y perdidos, la base de datos de documentos de viaje perdidos (1); y otro sistema informático para comprobar si hay avisos relacionados con documento de viaje (TDAWN). Asimismo, debemos tener en cuenta que determinados regímenes opresivos pueden incluir información sobre opositores políticos en estas bases de datos de Interpol para evitar que abandonen su país o para rastrear sus movimientos. Estas bases de datos se incluyen en los sistemas informáticos interoperables que está configurando la Unión Europea. En caso de que se realice una evaluación de protección internacional sobre una persona sujeta a una prohibición de entrada en espacio Schengen, ésta podrá obtener un visado de validez limitada, de conformidad con el artículo 25 del Código de visados[63]. Tal visado le permitirá cruzar la frontera exterior de la Unión Europea y le ofrecerá la posibilidad de solicitar protección internacional.

---

físico y retención/almacenamiento de datos. El legislador de la Unión Europea y los Estados miembros deben garantizar que la legislación en materia de sistemas informáticos interoperables no dé lugar a un incumplimiento de las normas de acceso incluidas en los instrumentos jurídicos que regulan los sistemas de información tradicionales.

[59] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Under watchful eyes: biometrics*, cit., pp. 49-58.

[60] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 18. Derecho de asilo. Se garantiza el derecho de asilo dentro del respeto de las normas de la Convención de Ginebra de 28 de julio de 1951 y del Protocolo de 31 de enero de 1967 sobre el Estatuto de los Refugiados de conformidad con el Tratado de la Unión Europea y con el Tratado de Funcionamiento de la Unión Europea.

[61] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 20. Igualdad ante la ley. Todas las personas son iguales ante la ley.

[62] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 21. No discriminación. 1. Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual. 2. Se prohíbe toda discriminación por razón de nacionalidad en el ámbito de aplicación de los Tratados y sin perjuicio de sus disposiciones particulares.

[63] Reglamento (CE) nº. 810/2009, del Parlamento y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados).

Como hemos visto anteriormente, el artículo 18 de la Carta de Derechos Fundamentales protege el derecho de asilo. El acceso efectivo a la protección internacional constituye también la base de la protección contra la devolución consagrada en el artículo 19[64] de la Carta de Derechos Fundamentales y en el artículo 78 del Tratado de Funcionamiento de la Unión Europea. En este contexto, compartir datos personales con terceros países puede dar lugar a riesgos particulares para las personas que necesitan protección internacional. Éstas pueden ser objetos de medidas de represalia, que abarcan desde sanciones penales al regresar a su país de origen, hasta medidas tales como la persecución de los miembros de su familia. Los instrumentos jurídicos que regulan los sistemas informáticos actuales prohíben generalmente compartir información con terceros países, con el fin de proteger la información acerca de los solicitantes de asilo en el espacio Schengen. Sin embargo, en determinadas circunstancias – generalmente con fines de devolución – los datos personales almacenados en sistemas de gestión de la información pueden ser compartidos con terceros países. En este tipo de casos, para evitar perjudicar a posibles solicitantes de asilo, la información normalmente sólo se comparte con el tercer país, una vez que ha finalizado el procedimiento de solicitud de asilo. Sin embargo, en circunstancias específicas, dicha información puede compartirse antes de que finalice el proceso de solicitud de asilo, por ejemplo, tras el rechazo de la solicitud por parte de la administración, pero cuando la solicitud aún esté pendiente de un recurso ante un tribunal. Este enfoque puede poner a los solicitantes de asilo en peligro. De modo que, en este tipo de casos, sería necesario revisar la normativa aplicable para evitar que se pongan en peligro a posibles solicitantes de asilo y/o a sus familias en sus países de origen[65]. Además, si los sistemas informáticos se hacen interoperables, la información contenida en las distintas bases de datos tradicionales podría utilizarse para confirmar la identidad alegada por un solicitante de asilo y reducir un posible riesgo de devolución – mientras se tramita su solicitud –.

Todos los sistemas informáticos desarrollados en la Unión Europea, excepto el SIS II y el ECRIS-TCN, contienen datos sobre personas, que no son sospechosas de haber cometido ningún delito. No obstante, las fuerzas y cuerpos de seguridad pueden acceder a los datos almacenados en Eurodac, SES y ETIAS-SEIAV, con el fin de luchar contra la delincuencia grave y/o el terrorismo, siempre que cumplan con los mecanismos específicos, contemplados en los instrumentos jurídicos que regulan el funcionamiento de dichos sistemas. Uno de estos mecanismos es el "sistema de cascada", que obliga a

[64] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 19. Protección en caso de devolución, expulsión y extradición. 1. Se prohíben las expulsiones colectivas. 2. Nadie podrá ser devuelto, expulsado o extraditado a un Estado en el que corra un grave riesgo de ser sometido a la pena de muerte, a tortura o a otras penas o tratos inhumanos o degradantes.

[65] Opinión n. 13 (FRA). Los Estados miembros de la Unión Europea deben adoptar todas las medidas necesarias para impedir que se comparta la información de un nacional de un tercer país que haya presentado una solicitud de protección internacional con terceros países. En el caso de rechazo de su solicitud de asilo, los Estados miembros sólo deben, en principio, compartir sus datos personales con las autoridades de terceros países, en caso de devolución, cuando la solicitud haya sido rechazada en última instancia y no pueda ser sujeto de un recurso ulterior.

los Estados miembros de la Unión Europea a consultar, en primer lugar, las bases de datos nacionales que estén directamente vinculadas a las investigaciones penales, y sólo después, se les concede el acceso a los sistemas informáticos a nivel europeo. Al consultar los sistemas informáticos de la Unión Europea, deben consultar el VIS antes de solicitar acceso a Eurodac, porque la información sobre solicitantes de asilo es particularmente sensible. De este modo, se garantiza que los conjuntos de datos sobre solicitantes de asilo, un grupo especialmente vulnerable ante posibles violaciones de sus derechos fundamentales, sólo se consulte como último recurso. El derecho de los niños a dicha protección y cuidado, necesarios para su bienestar, tal y como se establece en el artículo 24 de la Carta de Derechos Fundamentales, exige medidas específicas para prevenir futuras estigmatizaciones de los niños, en relación con posibles delitos que éstos pudieran haber cometido, en relación con procesos migratorios. Asimismo, el artículo 40[66] de la Convención sobre los derechos del niño exige prestar especial atención al trato proporcionado a los niños que supuestamente hayan cometido un delito, o a los que se les acuse o se reconozca la comisión de un delito. Según la Carta de Derechos Fundamentales, el interés superior del menor debe ser una consideración primordial. De modo que, considerando que los antecedentes penales pueden tener un efecto desproporcionado en el futuro desarrollo del niño, la Agencia de Derechos Fundamentales de la Unión Europea propone la posibilidad de que se excluya el acceso a la información policial almacenada en ECRIS-TCN que revele que un niño tiene antecedentes penales, o que se limite la disponibilidad de esta información a casos de delitos muy graves[67].

Además de cumplir sus propósitos específicos, la mayoría de sistemas de gestión de la información también contribuyen al control de la inmigración. De modo que, éstos pueden ser consultados para encontrar y detener a los migrantes en una situación irregular. Por ejemplo, el SES elaborará una lista de personas cuyo derecho de permanecer en el espacio Schengen ha expirado. Esta lista de los llamados "*overstayers*" se puede combinar con otros sistemas informáticos, lo que será un ejercicio fácil para los nuevos sistemas interoperables. En este contexto, la Agencia de Derechos Fundamentales de la Unión Europea ha puesto de relieve que ciertas prácticas de detención pueden afectar desproporcionadamente a los derechos fundamentales de los migrantes en situación irregular. Como consecuencia, la Agencia de Derechos Fundamentales de la Unión Europea desaconseja la detención de migrantes irregulares que estén haciendo uso de servicios esenciales, como es el caso de centros de salud o comisarías de policía[68]. De lo contrario, la interoperabilidad de los sistemas hará más

[66] Para más información acerca de los derechos de aquellos niños que sean sospechosos o estén acusados de haber cometido un delito, *vid.* Artículo 40. Convención sobre los derechos del niño.
[67] Opinión n. 15 (FRA). La Unión Europea y sus Estados miembros deben considerar la posibilidad de excluir el acceso a la información policial almacenada en ECRIS-TCN que revele que un niño tiene antecedentes penales, o limitar la disponibilidad de esta información a delitos muy graves.
[68] Opinión n. 16 (FRA). Se insta a los Estados miembros de la Unión Europea a que sigan aplicando las directrices del FRA de 2014 sobre detención de inmigrantes en situación irregular, prestando especial

difícil que los migrantes en situación irregular denuncien delitos ante la policía, ya sea como víctimas o testigos, ya que la policía vería automáticamente que se trata de un residente irregular y, en la mayoría de casos, estarían obligados por la legislación nacional a iniciar un procedimiento de expulsión/retorno. Si esto es así, al darse un mayor riesgo de detención, este fenómeno provocaría que los migrantes irregulares se mostrasen más reacios a denunciar posibles delitos ante la policía, contribuyendo a la impunidad de sus perpetradores.

Los errores en los sistemas informáticos utilizados en el ámbito de la gestión de solicitudes de asilo y la migración pueden tener consecuencias graves para las personas. Por ejemplo, debido a identificaciones erróneas, la policía puede llevar a cabo arrestos o los guardias fronterizos pueden denegar el cruce de la(s) frontera(s). En el caso de los solicitantes de asilo, éstos pueden ser sospechosos de haber intentado, intencionalmente, proporcionar una identidad falsa, afectando a la fiabilidad de toda su solicitud de asilo. Los estudios de la Agencia Europea de Derechos Fundamentales[69] muestran que los sistemas informáticos de la UE contienen datos alfanuméricos inexactos, como los nombres o fechas de nacimiento, debido a varias razones. De acuerdo con el RGPD y la Directiva de tratamiento de datos personales por parte de autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales[70], los Estados miembros de la Unión Europea tienen el deber de verificar la calidad de los datos personales antes de que se pongan a disposición del resto de usuarios de los sistemas informáticos. En este contexto, se aprecian esfuerzos significativos por parte de las distintas autoridades implicadas, entre los que podemos incluir las propuestas para reforzar el papel de eu-LISA en su labor de apoyo a los Estados miembros en la mejora de la calidad de los datos. No obstante, la Agencia de Derechos Fundamentales de la Unión Europea ha llamado la atención sobre la necesidad de evitar tener datos de baja calidad en los sistemas que puedan afectar negativamente a los derechos fundamentales de las personas[71]. Los datos biométricos

atención a los nuevos riesgos para los derechos fundamentales de los migrantes que la interoperabilidad pueda crear.

[69] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Under watchful eyes: biometrics*, cit., pp. 81-98.

[70] Directiva (UE) 2016/680, cit.

[71] Opinión n. 17 (FRA). El Consejo de la Unión Europea debe seguir incluyendo las cuestiones relativas a la calidad de los datos en las agendas de trabajo de los grupos de trabajo pertinentes para promover la redacción de directrices/protocolos de actuación para eu-LISA y el resto de actores. Estas directrices/protocolos deben incluir: en relación con los datos alfanuméricos, el desarrollo de directrices a escala europea sobre normas culturales, abordando cuestiones como las transliteraciones, distintas nomenclaturas, distintas formas de registrar la edad en relación con las fechas de nacimiento y los distintos calendarios. Estas directrices contribuirían a mejorar la calidad de los datos; en relación con los datos biométricos, la revisión de las normas de calidad de las huellas dactilares almacenadas en VIS, teniendo en cuenta que las huellas dactilares de los solicitantes de asilo también pueden coincidir con el VIS para determinar el Estado miembro responsable de tramitar sus reclamaciones en el marco del sistema de Dublín; una colección de buenas prácticas administrativas para limitar los errores, como el uso de lectores electrónicos, los criterios de búsqueda y la simplificación de procedimientos; una serie de mecanismos técnicos que reduzcan el riesgo de errores, como la verificación automática en varias sistemas informáticos cuando se introduzcan datos, y la posibilidad de utilizar búsquedas fonéticas;

conectan a una persona con los datos alfanuméricos almacenados en un sistema de gestión de la información. La calidad de los identificadores biométricos es, por tanto, de suma importancia. Aunque es poco frecuente, las investigaciones de campo de la Agencia de Derechos Fundamentales de la Unión Europea han revelado incidentes individuales de solicitudes de asilo que se han llevado a cabo sobre la base de coincidencias biométricas erróneas[72]. En la actualidad, los estándares de calidad del registro de huellas dactilares en Eurodac, que posee principalmente datos personales sobre solicitantes de asilo, son superiores a los estándares de calidad de recopilación de datos biométricos en VIS. Esto se debe a que en el sistema VIS, cada Estado miembro es responsable de controlar la calidad, mientras que para Eurodac, el responsable – de forma centralizada – es eu-LISA. Sin embargo, las huellas dactilares recogidas para Eurodac pueden ser contrastadas con VIS para ver si el solicitante ha solicitado un visado en el pasado. Con la implementación de la interoperabilidad de los sistemas, el identificador biométrico de una persona se conecta a la información contenida en todos los sistemas informáticos, independientemente del estándar de calidad que se utilizó para registrarse. También se prevé que la interoperabilidad incluya medidas para mejorar la presentación de informes y la recopilación de estadísticas, lo que mejoraría la calidad de los datos. Asimismo, como hemos indicado anteriormente, la calidad de los datos también puede verse afectada debido al desarrollo físico de una persona, lo que reduce la fiabilidad del reconocimiento y cruce de datos, en función de los datos biométricos, especialmente tras el transcurso de largos períodos de tiempo. Las autoridades nacionales y los expertos atribuyen un alto grado de credibilidad a los datos biométricos, y el tratamiento de estos datos es técnicamente complejo. Por este motivo, resulta difícil que las personas interesadas puedan inducir a error a los sistemas informáticos y, al mismo tiempo, resulta difícil poder demostrar que se ha generado una coincidencia biométrica de forma errónea. En este tipo de casos, la investigación de la Agencia de Derechos Fundamentales de la Unión Europea muestra que los errores pueden darse cuando, por ejemplo, las huellas dactilares de una persona están erróneamente vinculadas a los datos alfanuméricos de otra persona[73].

Por último, conviene señalar que el artículo 8.2 de la Carta de Derechos Fundamentales, así como la normativa en materia de protección de datos de la Unión Europea[74], prevén el derecho de acceso, corrección y supresión de los datos

---

mejorar la recopilación de estadísticas sobre datos inexactos y de baja calidad. La Comisión europea debe incluir cuestiones de calidad de datos en las evaluaciones de Schengen para asegurar la aplicación de las recomendaciones y mejores prácticas desarrolladas por eu-LISA. Los Estados miembros de la Unión Europea también deben mostrar especial atención a la calidad de los datos almacenados, si éstos se transfieren a los sistemas informáticos de la Unión Europea. Deberían, por ejemplo, desarrollar procedimientos estandarizados para la verificación de los datos almacenados en los sistemas nacionales de gestión de la información.

[72] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Under watchful eyes: biometrics*, cit., pp. 99-106.

[73] *Ibidem.*

[74] Para un estudio más detallado sobre el derecho de acceso, corrección o eliminación de datos, *vid*., Reglamento (UE) 2016/679, cit. Artículo 5. Principios relativos al tratamiento.

almacenados. A pesar de los frecuentes problemas de calidad de los datos, las quejas acerca del uso incorrecto o ilegal de los datos son poco frecuentes. Esto podría deberse a que existe una falta de comprensión y conocimiento de cómo ejercer el derecho de acceso, corrección o eliminación de los datos inexactos que se almacenan. La naturaleza engorrosa de estos procesos, los obstáculos administrativos, las barreras del idioma y la falta de abogados especializados también explican por qué pocas personas tratan de ejercer estos derechos. Según las constataciones de la Agencia de Derechos Fundamentales de la Unión Europea[75], lo procedimientos complicados y los obstáculos administrativos y de lenguaje pueden impedir en la práctica que las personas interesadas ejerzan su derecho de acceso, rectificación o supresión. Estos procedimientos podrían revisarse al implementarse la interoperabilidad entre los distintos sistemas. El establecimiento de un "procedimiento de ventanilla única" para recibir solicitudes de acceso, corrección y supresión de datos podría servir para que se simplificaran los procedimientos.

[75] FRA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Under watchful eyes: biometrics*, cit., pp. 81-98.

6. Conclusiones

En los últimos años, la crisis migratoria y los atentados terroristas cometidos en varios Estados miembros han puesto de manifiesto la necesidad de reforzar las fronteras exteriores de la Unión Europea. En este contexto, la UE ha propuesto una serie de medidas concretas para salvaguardar la seguridad de Europa: una fuerte inversión en la Agencia de la Guardia de Fronteras y Costas; un sistema de información de Schengen mejorado; comprobaciones sistemáticas en las bases de datos pertinentes de todas las personas que crucen las fronteras exteriores; un nuevo Sistema de Entradas y Salidas para los nacionales de terceros países; el Sistema Europeo de Información y Autorización de Viajes y nuevas iniciativas destinadas a que las bases de datos de la Unión Europea sean interoperables. Estas medidas han sido acogidas con cierto recelo por parte de determinados Estados miembros, que detectan otras prioridades en la asignación de fondos en el presupuesto para el periodo 2021-2027. Así como, por parte de un gran sector de la sociedad civil que se plantea si se van a garantizar (o no) los derechos humanos de las personas migrantes.

Como hemos podido comprobar, las autoridades de la Unión Europea utilizan varias bases de datos en su lucha contra la delincuencia, el control de fronteras y la gestión de los flujos migratorios. Entre éstas, destacan: el SIS II, que permite que las autoridades nacionales encargadas de realizar los controles pertinentes, tanto en la frontera exterior de Schengen como dentro del espacio Schengen, hagan circular alertas sobre personas buscadas o desaparecidas y objetos como documentos y vehículos robados; el VIS, que permite a los guardas fronterizos verificar si la persona que presenta un visado es su titular legítimo; Eurodac, la base de datos de huellas dactilares de solicitantes de asilo en la Unión Europea; el SES, que registra la entrada y salida de los nacionales de terceros países que viajan a la Unión Europea; y el ETIAS-SEIAV, que se plantea con el fin de llevar a cabo controles sobre los viajeros, exentos de visado, que se disponen a viajar a territorio europeo.

La Unión Europea está tratando de mejorar estos sistemas de información con el fin de mejorar la efectividad y la eficiencia de los controles en las fronteras exteriores; contribuir a la prevención de la inmigración ilegal y la lucha contra ella; contribuir a un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión Europea, lo que incluye el mantenimiento de la seguridad pública y el orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros; mejorar la aplicación de la política común de visados; ayudar a examinar las solicitudes de protección internacional; contribuir a la prevención, detección e investigación de los delitos de terrorismo o de otros delitos penales graves; y ayudar a identificar a las personas desconocidas que no puedan identificarse o a los restos humanos sin identificar en caso de catástrofes naturales, accidentes o atentados terroristas.

En esta línea de trabajo, el pasado 20 de mayo de 2019, se aprobaron los Reglamentos (UE) 2019/817 y (UE) 2019/818, relativos al establecimiento de un marco jurídico que permita la interoperabilidad de los sistemas de información de la Unión

Europea en el ámbito del control de sus fronteras exteriores, a través de cuatro grandes novedades: el Portal Europeo de Búsqueda, que permite la búsqueda simultánea en varios sistemas de información de la UE y proporciona una "ventanilla única" (en una sola pantalla de ordenador) para todos los resultados de la comprobación de documentos; el servicio de coincidencia biométrica compartida, que habilita la consulta y la comparación de identidades múltiples; el Repositorio Común de Identidad, que proporciona información bibliográfica y biométrica básica, como nombres y fechas de nacimiento de ciudadanos no pertenecientes a la Unión Europea, para que puedan identificarse eficazmente y, por último, el Detector de Identidad Múltiple, que ayuda a establecer si hay diferentes nombres que pertenecen a la misma identidad y alertan a los guardias fronterizos y a los casos policiales en caso de actividad fraudulenta.

Pero, no se trata de una tarea sencilla, pues dicho marco normativo se enfrenta a una serie de retos, tales como: garantizar la identificación correcta de las personas; contribuir a luchar contra la usurpación de identidad; mejorar la calidad de los datos y armonizar los requisitos de calidad de los datos almacenados en los sistemas de información de la Unión Europea, respetando al mismo tiempo los requisitos de tratamiento de datos de los instrumentos jurídicos que rigen los diferentes sistemas y las normas y principios en materia de protección de datos; facilitar y apoyar la aplicación técnica y operativa por parte de los Estados miembros de los sistemas información de la Unión Europea; reforzar, simplificar y uniformizar las condiciones de seguridad de los datos y de protección de datos que rigen en los respectivos sistemas de información de la Unión Europea, sin perjuicio de la protección y las salvaguardias especiales otorgadas a ciertas categorías de datos; racionalizar las condiciones de acceso de las autoridades designadas al SES, al VIS, al SEIAV y a Eurodac, garantizando al mismo tiempo las condiciones necesarias y proporcionadas para dicho acceso; y apoyar los objetivos del SES, el VIS, el SEIAV, Eurodac, el SIS y el ECRIS-TCN.

Este nuevo sistema integrado de gestión de la información debe ofrecer una serie de garantías a la población migrante, tal y como se contempla en los distintos instrumentos regionales. En el ámbito del Consejo Europa, tanto los derechos garantizados en el Convenio para la protección de las personas en lo que respecta al tratamiento automático de sus datos personales, como los derechos contemplados en el Convenio Europeo de Derechos Humanos. Asimismo, en el ámbito de la Unión Europea, tal y como hemos visto a lo largo de este artículo, deberán garantizarse tanto los derechos contemplados en la normativa específica en materia de protección de datos, como los derechos garantizados en la Carta de Derechos Fundamentales, entre los que podemos destacar: el respeto a la dignidad humana (artículo 1 CDDFF), la protección de los datos personales (artículo 8 CDDFF), el derecho de asilo (artículo 18 CDDFF), así como la protección en caso de expulsión, expulsiones o extradición (artículo 19 CDDFF), el derecho de igualdad ante la ley (artículo 20 CDDFF), el derecho a la no discriminación (artículo 21 CDDFF), así como los derechos del niño (artículo 24 CDDFF).

En este contexto, la capacidad de las autoridades de control de fronteras para recoger información, especialmente para hacer el seguimiento de posibles indicios de

ataques terroristas y evaluar la amenaza terrorista en general, será de suma importancia. No obstante, será determinante que las soluciones de interoperabilidad se diseñen y desarrollen garantizando una serie de estándares mínimos. Entre éstos, debemos destacar: el derecho a la información, que debe abarcar todos los fines del tratamiento de datos en los sistemas informáticos en el ámbito de la gestión del asilo y la migración, teniendo en cuenta la edad, género y cultura del viajero/migrante (1); las autoridades fronterizas deben evitar el uso de la fuerza ante una posible negativa en el registro de huellas dactilares, así como se debe tener en cuenta que ejercer presión sobre el migrante podría dar lugar a una re-victimización – pudiendo tratarse de posibles víctimas de tortura, violencia sexual o de género o víctimas de otros delitos graves – y sólo debe utilizarse la privación de libertad como una medida excepcional en este tipo de casos (2); las autoridades fronterizas no deben utilizar nunca la fuerza contra niños ni privarlos de su libertad para obtener sus huellas dactilares, sino que deben centrarse en tratar de establecer una relación de confianza con el niño (3); las autoridades competentes deben registrar sistemáticamente a los niños desaparecidos en los sistemas de gestión de la información y deben establecerse mecanismos eficaces de cooperación entre la policía y las autoridades de protección de la infancia, así como entre los tutores de los menores (4); la UE y sus Estados miembros deben exigir a los diseñadores de estos sistemas informáticos que se involucre a expertos en protección de datos personales y expertos en derechos fundamentales en el diseño y desarrollo del software (5); las instituciones de la UE y los Estados miembros deben establecer todas las medidas necesarias para evitar cualquier tipo de acceso ilegal a los datos almacenados en los sistemas informáticos en el ámbito del asilo y de la (in)migración (6); la credibilidad de los solicitantes de asilo no debe verse socavada por la presunción de que su incapacidad para poder registrar sus huellas dactilares, o sólo para poder registrar huellas dactilares de baja calidad (debido a posibles lesiones) se derive de una falta de voluntad de proporcionar sus huellas y/o el deseo de ocultar su identidad (7); las autoridades competentes deberían adoptar todas las medidas necesarias para impedir que la información relativa a la presentación de una solicitud de asilo se comparta con un tercer país y, en caso de que se haya rechazado la solicitud, ésta no debería compartirse hasta que haya sido rechazada en la última instancia (8); las autoridades competentes deben evaluar cuidadosamente cómo el acceso de las fuerzas del orden a los datos puede afectar a los derechos fundamentales de los usuarios, a través de mecanismos y/o protocolos de actuación, tales como el "sistema en cascada" (9); las autoridades competentes deberían evaluar cómo la interoperabilidad puede afectar a la detención y/o devolución de los (in)migrantes en situación irregular, que se encuentran haciendo uso de servicios básicos como puede ser la sanidad, o la denuncia de un delito como víctima o testigo en una comisaría de policía (10); las instituciones de la UE deben desarrollar guías prácticas acerca de cómo deben registrarse los datos alfanuméricos (teniendo en cuenta que, por ejemplo, una misma fecha de nacimiento puede tener varias formas de registro, atendiendo al país o a la cultura) y biométricos (estableciendo estándares mínimos de calidad de los datos), con el fin de poder evitar

posibles errores (11); y las autoridades competentes deben garantizar el derecho de acceso, corrección y supresión de los datos personales de los usuarios (12).

Y es que, en pleno Siglo XXI, la cuestión de la implementación de las denominadas fronteras inteligentes es una cuestión global, que afecta tanto a la Unión Europea, como al resto de Grandes Potencias (Estados Unidos, China, etc.) y su utilidad para tratar de salvaguardar la seguridad en nuestras fronteras parece innegable. No obstante, es en esta fase de experimentación, en la que la UE debe plantearse cómo podemos servirnos de estas nuevas tecnologías, garantizando los derechos humanos de todas y cada una de las personas que traten de cruzar nuestras fronteras.

RESUMIEN: La crisis migratoria y los atentados terroristas cometidos en varios Estados miembros han puesto de manifiesto que para abordar los retos en materia de migración, terrorismo y delincuencia es fundamental invertir en la mejora de los sistemas de gestión de la información utilizados en los controles fronterizos. Hasta ahora, éstos estaban estrictamente separados, fragmentados y desconectados. Por este motivo, la Unión Europea ha aprobado, recientemente, un marco legislativo para garantizar su interoperabilidad. Una iniciativa que trata de prevenir, de forma más eficaz, posibles amenazas terroristas y delitos relacionados con la migración – como es el caso de la trata de personas –, pero que, al mismo tiempo, debe respetar la protección de datos y el derecho a la privacidad de aquellas personas que cruzan nuestras fronteras.

KEYWORDS: interoperabilidad – sistemas – gestión – información – Schengen.

COMPUTER PROCESSING DATA AND PROTECTION OF FUNDAMENTAL RIGHTS IN THE EXTERNAL BORDERS OF THE EUROPEAN UNION

ABSTRACT: The migration crisis and terrorist attacks committed in several Member States have shown that in order to address the challenges of migration, terrorism and crime, it is essential to invest in the improvement of the information management systems used in border controls. Until now, these were strictly separated, fragmented and disconnected. For this reason, the European Union has recently approved a legislative framework to guarantee its interoperability. An initiative that tries to prevent, in a more effective way, possible terrorist threats and crimes related to migration – such as human trafficking – but which, at the same time, must respect data protection and the right to the privacy of those people who cross our borders.

KEYWORDS: interoperability – systems – management – information – Schengen.