

# LA INTEROPERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN EUROPEOS APLICACIÓN OPERATIVA E INTEGRACIÓN TÉCNICA PARA LA GUARDIA CIVIL

FRANCISCO PULIDO CATALÁN

TENIENTE CORONEL JEFE DE LA COMANDANCIA DE HUESCA. DOCTORANDO EN DERECHO DE LA UNED EN EL PROGRAMA DE DERECHO Y CIENCIAS SOCIALES

Fecha de recepción: 09/03/2022. Fecha de aceptación: 14/03/2022

## RESUMEN

La aprobación el 20 de mayo de 2019 de los dos Reglamentos europeos conocidos como de la interoperabilidad de los sistemas de información europeos supone la culminación de un largo proceso político y legislativo, para favorecer el acceso y explotación integrada de los sistemas de información del espacio de libertad, seguridad y justicia (ELSJ) por las autoridades competentes nacionales en materia de seguridad pública de los Estados Miembros (EE.MM).

La importancia estratégica para la Guardia Civil de disponer y consumir de forma automatizada nuevas fuentes de información en la prevención y mantenimiento de la seguridad ciudadana redundará en una mayor eficacia en la prestación del servicio público del Cuerpo. Teniendo en cuenta que el plazo previsto para la implantación nacional de la interoperabilidad concluye a finales del año 2023, resulta imprescindible impulsar las medidas necesarias que garanticen la integración de los sistemas interoperables en las plataformas operativas del Cuerpo.

*Palabras clave:* interoperabilidad, sistemas, información, integración, seguridad, Guardia Civil.

## ABSTRACT

On 20 may 2019 the so called European Regulations on information systems interoperability were adopted. The two new lawmaking entail the culmination of a long political and legislative process to facilitate the integrated access and exploitation of the european information systems of the Freedom, Security and Justice Area (AFSJ) by the law enforcement competent authorities in the Member States (MS).

It is considered of strategic institutional relevance to get automatized access and usage to new sources of information in preventing and keeping people security. The further exploitation of the newly information recorded will bring added value when carrying the police functions assigned to the Guardia Civil. Having regard the deadline foreseen for the national implementation of the interoperability by the end of 2023, it is crucial to foster the necessary measures to guarantee the successful integration of the interoperable information systems in the operational platform of the Guardia Civil.

*Keywords:* Interoperability, systems, information, integration, security, Guardia Civil.

## 1. EL IMPULSO EUROPEO EN LA MEJORA DE LOS SISTEMAS DE INFORMACIÓN

La interoperabilidad aparece como requisito tecnológico que propicie el fomento del intercambio y la compartición de información en el Programa de la Haya para la consolidación del espacio de libertad, seguridad y justicia. Si bien, la interoperabilidad que predica no se limita a los sistemas de información europeos, sino que también manifiesta lo propio entre los sistemas nacionales, e incluso entre los nacionales y los europeos, con lo que parece deslizar que los EE.MM deber proceder a integrar sus sistemas de información antes de proceder a hacer lo propio con los europeos (COM(2005) 184 final, 2005). Resulta sorprendente que la interoperabilidad ya no aparece en el Plan de acción del Consejo y de la Comisión por el que se aplica el Programa de la Haya publicado tan solo tres meses después.

Si bien es la propia Comisión la que posteriormente delimita el alcance de la interoperabilidad y lo circunscribe exclusivamente a propiciar mejoras en los sistemas de información europeos para que puedan “apoyar más eficazmente las políticas relacionadas con la libre circulación de personas y contribuir al objetivo de luchar contra el terrorismo y la delincuencia grave” (COM(2005) 597 final, 2005). Siendo una comunicación monográfica, la Comisión por primera vez incluye una propia definición de interoperabilidad de los sistemas de información europeos destinada a promover el intercambio y la compartición de información que se configura como un derecho a ejercitar por los EE.MM, amparado en el principio de disponibilidad de la información. Así define la interoperabilidad como la “capacidad para compartir e intercambiar información y conocimientos de los sistemas de tecnologías de la información y las comunicaciones (TICs) y de los procesos empresariales en que se basan”.

La proyección expansiva de los sistemas de información europeos pasa así a convertirse en el centro de gravedad del debate político, tanto por la capacidad de sus prestaciones como por sus potenciales usuarios. La misma Comunicación de la Comisión europea mencionada anticipa la posibilidad legal de ampliar el acceso a los sistemas de información europeos a las autoridades competentes de los EE.MM, en materia de lucha contra el terrorismo y la delincuencia organizada, si bien los circunscribe a las categorías de datos almacenados compatibles con las descripciones establecidas en los instrumentos jurídicos europeos de creación de los sistemas de información. De esta forma ilustra que las autoridades competentes en materia de seguridad interior, quiere decir las Fuerzas y Cuerpos de Seguridad (FCS) y los servicios de inteligencia de los EE.MM, podrían tener acceso al Sistema de Información Schengen de segunda generación (SIS II), exclusivamente a los datos almacenados referidos a individuos sobre los que pesa una prohibición de entrada temporal en el espacio Schengen introducida por algún EE.MM, en base a incumplimiento de la legislación interna de inmigración, o sobre el que se ha introducido un señalamiento que representa una amenaza para el orden público o la seguridad nacional<sup>1</sup>.

No obstante, la citada Comunicación critica la infra explotación y heterogeneidad de la utilización de los sistemas de información, precisamente en aquellas categorías de datos que se corresponden directamente con competencias de seguridad interior de los EE.MM en el ejercicio de actuaciones de prevención, detección e investigación

1 Curtin, Deirdre “La Seguridad del intersticio y la compartición de datos interoperables. Un primer corte”, p. 69, <https://www.ceps.eu/publications/constitutionalising-security-union-effectiveness-rule-law-and-rights-counteracting>

de infracciones penales (particularmente para la lucha contra el terrorismo, como son los individuos para los que se introduce señalamiento personales a efectos de vigilancia discreta o control específico), así como también la falta de inclusión de datos biométricos estipulados en el sistema de información europeo para la comparación de las impresiones dactilares (EURODAC) que podrían contribuir a identificar, de forma indubitada, amenazas concretas a la seguridad de la Unión Europea (UE) e incluso motivar denegaciones de asilo en otros EE.MM. Entendemos que la Comisión lanza un reproche a los EE.MM aglutinados en torno al Consejo por no predicar con el mismo énfasis el acceso por parte de las autoridades competentes en materia de inmigración (EURODAC) y visados (Sistema de información de visados, VIS) respecto de los sistemas de información instituidos para las finalidades de cooperación policial en las descripciones correspondientes (SIS II) que redundaría en beneficio del ejercicio de sus competencias.

A pesar de las dificultades y disputas expresadas, parecía que la interoperabilidad de los sistemas de información europeos se estaba abriendo paso para posibilitar una mayor capacidad de consulta de datos que estimularía a medio plazo el incremento significativo de intercambio y compartición de información (Consejo JAI 8857/03, 2003). Sin embargo, el Supervisor europeo de Protección de datos consideró notoriamente lesiva a la normativa de protección de datos personales las propuestas que contenía la citada Comisión.

En este sentido se mostró especialmente beligerante con el concepto técnico de la noción de interoperabilidad introducido por la Comisión, desprovisto de fundamentación jurídica suficiente, argumentando que dicho criterio desbordaba la limitación de la finalidad legal prevista establecida en la creación de cada sistema de información europeo, así como también la justificación de acceso policial a bases de datos con finalidad de gestión meramente administrativa, dotadas de salvaguardas de protección inferiores que aquellas con finalidad policial. No debemos olvidar que el objetivo de la mejora del intercambio de información propugnado en el Programa de la Haya contemplaba la adopción de medidas necesarias para garantizar la protección de datos, que se concretó mediante una propuesta legislativa en materia de protección de datos que acompañara a la propuesta correspondiente del desarrollo jurídico del principio de disponibilidad.

El capítulo 3.1 del Plan de Acción del Consejo y la Comisión por el que se aplica el Programa de la Haya, adoptado por el Consejo de Justicia e Interior de 2 y 3 de junio de 2005, confirmó la presentación de tal propuesta legislativa para 2005, junto con una Propuesta sobre garantías adecuadas y vías de recurso eficaces para la transferencia de datos personales a efectos de cooperación policial y judicial en asuntos penales.

Si bien consideramos que la propuesta de la Comisión adolecía de una mayor fundamentación y análisis prospectivo que estableciera una hoja de ruta de interoperabilidad para su consecución, no es menos cierto que, tan rotunda y amplia censura del Supervisor Europeo de Protección de Datos, advirtiendo de graves infracciones de derecho comunitario, consiguió que se abandonara el proyecto de interoperabilidad, al menos su concepción primigenia de sistemas de información capaces de intercambiar y/o compartir información entre sí directamente disponibles para su utilización posterior por los usuarios de los mismos.

Sin embargo el empeño en la interoperabilidad continuó, aprovechando la Comunicación del consejo mencionada anteriormente sobre el marco europeo de la interoperabilidad, en la que se expresaba la viabilidad técnica de la interoperabilidad de los sistemas de información europeos existentes y futuros, si bien considera que sería conveniente su gestión integrada en una sola estructura organizativa (propone la Agencia Europea de Fronteras) que aglutinara las aplicaciones de acceso y consulta, manteniendo disociados tanto el almacenamiento de los datos de cada sistema como el flujo de las comunicaciones de consulta de los mismos almacenados en cada sistema de información.

Tuvo que transcurrir más de una década para que el concepto de interoperabilidad de los sistemas de información fuese de nuevo recuperado y presentado como una de las prioridades de la UE en el ELSJ, pero esta vez adaptado al tamiz de las experiencias anteriores, como sostiene Tomaszycycki, 2018 “la interoperabilidad es la capacidad de varios sistemas y organizaciones para participar en una cooperación efectiva basada en: (1) estándares técnicos, (2) regulaciones legales y (3) medidas organizacionales”.

Una vez analizado el origen de la interoperabilidad de los sistemas de información europeos consideramos oportuno continuar cronológicamente el análisis de los avances producidos en materia de intercambio de información en los epígrafes siguientes hasta alcanzar la fecha que nos permita simultanear ambos asuntos. La evolución posterior de la “interoperabilidad” se abordará con más detalle en epígrafes posteriores, por lo que en el presente capítulo nos referiremos a la interoperabilidad como la capacidad de los sistemas de información y sus componentes para interactuar basándose en el uso de las TICs.

## **2. LA HOJA DE RUTA HACIA LA INTEROPERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN EUROPEOS**

La adopción en el Consejo de ministros de Justicia e Interior de la UE del 6 de junio de 2016 de la denominada “Hoja de ruta para mejorar el intercambio y la gestión de la información, con inclusión de soluciones de interoperabilidad en el ámbito de la Justicia y los Asuntos de Interior, (Consejo 9368/1/16, 2016), marca un antes y un después en la evolución del intercambio y la compartición de información policial en Europa. La posibilidad de que las agencias policiales y de seguridad de los EE.MM puedan acceder en consulta a los datos alojados en los sistemas de información europeos en el ejercicio de sus funciones de prevención e investigación de los delitos de terrorismo y de la delincuencia organizada supone una auténtica revolución al ampliar el acceso a una mayor cantidad de información que a su vez generará un incremento significativo del intercambio de información entre dichas agencias, y también eventualmente con Europol, redundando en mayores cotas de seguridad en la UE.

Sin embargo la presentación de la hoja de ruta por la Presidencia holandesa de turno de la UE no puede considerarse en modo alguno una iniciativa improvisada o imprevista, sino que supone la culminación de una colaboración institucional fraguada a través de la Comunicación previa de la Comisión europea (COM (2016) 205 final, 2016), las Conclusiones del Consejo JAI de 18 de diciembre del 2015 y el impulso interinstitucional del Coordinador de la lucha contra el terrorismo de la UE.

En efecto, el desarrollo en la década anterior de los instrumentos jurídicos europeos que propiciaron el intercambio de información al que nos hemos referido, en los capítulos anteriores, fue gradualmente evolucionando a través de la presentación de iniciativas de armonización conceptual, técnica y operativa de las reglas de procedimiento operativo del funcionamiento de los sistemas de información que permitieran un mayor y mejor aprovechamiento de las posibilidades de intercambio de información de dichos instrumentos. Sin lugar a dudas, la creación y puesta en funcionamiento en su día de la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (EU-LISA), a quien le corresponderá tutelar el proceso de implantación de la interoperabilidad europea, contribuyó decididamente a la presentación de la hoja de ruta (Reglamento (UE) 1077/2011).

La centralización de los sistemas de información policiales europeos en el seno de una Agencia europea ha supuesto la externalización de la gestión operativa y el mantenimiento de los sistemas de información europeos y de su infraestructura de comunicaciones soporte por parte de la Comisión europea y, por ende, la profesionalización técnica, administrativa y económico-financiera de dicha gestión. Consideramos que la capacitación profesional de la Agencia EU-LISA junto con la dirección de la estructura administrativa y técnica independiente típica de las agencias europeas, (Dausà, Mariona, 2021) constituye suficiente aval para garantizar que la implantación de la interoperabilidad de los sistemas de información sea una realidad pronto y, “como sostiene Zoltán, Dóczy (2013), proporciona notables ventajas”<sup>2</sup>.

### **3. EL CONTENIDO DE LOS REGLAMENTOS EUROPEOS DE INTEROPERABILIDAD**

La regulación de la interoperabilidad de los sistemas de información europeos se halla contenida en dos reglamentos distintos, los reglamentos 2019/817 y 2019/818 como consecuencia de su correspondencia con bases jurídicas distintas del Tratado de Funcionamiento de la Unión Europea (TFUE). Mientras ambos reglamentos refieren a los artículos 16 (2) y 74 del TFUE, el reglamento 2019/817 encuentra su base jurídica en el art.72 (2), a), b), d) y e), que corresponde a la cooperación en materia de gestión de fronteras y visados, y el Reglamento 2019/818, está basada en los artículos 78 (2) e), 79(2)c), 82(1)d), 85(1), 87(2)a) y 88(2) TFUE que se corresponde con la cooperación en materia policial y judicial, asilo y migración.

Ambos reglamentos establecen una arquitectura de acceso y consulta a los sistemas de información interoperables secuencial, en dos etapas, garantizando, al mismo tiempo, tanto la legitimidad y licitud de la consulta como la integridad de la respuesta obtenida. Para hacerlo posible, las disposiciones reglamentarias han establecido un complejo diseño de sistemas de interconexiones previas de acceso a datos de carácter instrumental que permiten anticipadamente auditar y validar las búsquedas realizadas a través de la creación de una serie de componentes que configuran la arquitectura de interoperabilidad.

2 DÓCZI, ZOLTÁN, “The Development, the Integration and the Assessment of the Existing Large-Scale IT Systems in the Area of Freedom, Security and Justice”, Acta juridica hungarica 54, No 2, pp. 164–183 (2013) p.182.

De esta forma, el capítulo segundo de los reglamentos establece la creación del Portal Europeo de Búsquedas (PEB/ESP en inglés) como la interfaz única de búsqueda simultánea en todos los sistemas interoperables que proporcionaría el resultado de la coincidencia existente en cualquiera de los sistemas de información que formarán parte de la interoperabilidad, esto es el Sistema de entradas y salidas (SES), el VIS, el Sistema de información sobre autorizaciones de viajes (SEIAV), EURODAC, SIS II y el Sistema Europeo de Información de Antecedentes Criminales para ciudadanos de terceros países (ECRIS-TCN).

El capítulo tercero establece la creación del Servicio de correspondencia biométrica compartido (SCB/BMS acrónimo en inglés) que alojará los formularios de datos biométricos que corresponden a las identidades de los individuos registrados en alguno de los sistemas de información interoperables que almacenan datos biométricos.

El capítulo cuarto dispone la creación del Registro Común de datos de identidades (RCDI/CIR acrónimo en inglés), que contendrá una ficha individual de datos de identidad de cada individuo registrado en los sistemas interoperables, a excepción del SIS II (ya que el CIR/RCDI lo que hace es “resumir” las identidades de los sistemas de información que solo recogen datos de ciudadanos extranjeros, puesto que el SIS incluye de todos, siendo perfectamente usable para identificar al ser un sistema puramente policial, en contraposición con el carácter administrativo principal, y ahora secundario, policial del resto de sistemas).

El capítulo cinco establece la creación de un Detector de identidades múltiples (DIM/MID, acrónimo en inglés) para facilitar el cruce de datos de identidad y biométricos de los sistemas interoperables que poseen ambos tipos de registros con los datos del RCDI y del SIS II (las identidades alojadas no se comparten con el RCDI) y poder detectar la identidad real entre las posibles registradas.

### 3.1. FUNCIONAMIENTO PRÁCTICO DE LAS BÚSQUEDAS Y CONSULTAS DE INTEROPERABILIDAD

Para explicar el funcionamiento práctico de la interoperabilidad resulta indispensable recordar las categorías de datos alojados y finalidad de cada uno de los sistemas de información interoperables y el tipo de consultas que podrán realizar las autoridades nacionales designadas, según se trate de autoridades competentes con dicha finalidad o no.

La consulta inicial se hará en el PEB que, si se trata de datos alfanuméricos, consultará el RCDI, que en caso de que existan coincidencias de datos biométricos asociados (solo posible respecto del SES, VIS y EURODAC), automáticamente examinará la SCB que determinará el sistema de información que contiene los datos biométricos asociados a la identidad alfanumérica consultada y, en el caso de que existan más identidades asociadas a esos datos biométricos, el RCDI creará un vínculo en el DIM que enviará una alerta a la oficina española para la solicitud de información complementaria a la entrada nacional (SIRENE) quien remitirá a la autoridad competente nacional, que creó o modificó el señalamiento, para que resuelva la multiplicidad de identidades (identidades fraudulentas o cambios identidad legal). En caso de que la consulta se inicie a través de datos biométricos, automáticamente el PSB consultará directamente con el SCB en el que se compararán las fórmulas de los algoritmos, muestra y alojados.

Los reglamentos de interoperabilidad remiten la gestión y control de los accesos y consultas del funcionamiento e interconexiones entre los componentes de la interoperabilidad a los órganos nacionales instituidos conforme lo dispuesto en los propios reglamentos de los sistemas de información interoperables. Esto es, la creación a nivel nacional de la figura de Autoridad Nacional (AN) que facilitaría los accesos a las autoridades competentes conforme a la finalidad del sistema en concreto, que, en el caso del SES serían, las “autoridades de inmigración”. Además también se creará uno o varios Punto de Acceso Central (PAC) en cada EE.MM, que serían los encargados de facilitar y auditar las consultas que realicen las “autoridades designadas” con fines de prevención, detección e investigación de delitos graves y terrorismo en los casos establecidos.

Por tanto, en el caso de las consultas de las reconocidas como autoridades de inmigración, a efectos de identificación de un extranjero, el agente de la Guardia Civil, investido de su condición de agente de la autoridad y perteneciente a una unidad del Cuerpo que figura como autoridad designada, podrá realizar la consulta con datos biográficos y biométricos, accediendo a un “resumen” de los datos de identidad contenidos en los cuatro sistemas consultados, pero sin que señale el o los sistemas de información de procedencia de los datos.

Por su parte, en el caso de consultas de investigación, prevención detección o enjuiciamiento de delitos graves y de terrorismo, el agente de la Guardia Civil que figure como autoridad designada, y en el marco de una investigación penal por delitos graves y terrorismo, podrá realizar también la consulta con datos biográficos o biométricos y el sistema solo devolvería el dato señalando el sistema de información concreto en el o los que existen registros del individuo objeto de búsqueda. Si el agente dispone de habilitación para acceder a dicho sistema o sistemas, podrá acceder así a la información alojada en una segunda etapa. Esta búsqueda para investigación excluye claramente las consultas contra ECRIS-TCN.

### 3.2. EL SISTEMA DE GOBERNANZA EUROPEO DE LA INTEROPERABILIDAD

El funcionamiento ágil, eficaz y correcto de la interoperabilidad descansa en el óptimo ejercicio de una responsabilidad compartida entre los EE.MM y la Comisión Europea en calidad de garante, tanto de su adecuada operatividad como de la legitimidad de su utilización por las distintas autoridades designadas de los EE.MM.

Desde el punto de vista de la adecuación de la utilización de la interoperabilidad a las finalidades previstas en los reglamentos de interoperabilidad, los distintos instrumentos jurídicos de los sistemas de información interoperables contienen numerosas disposiciones que establecen mecanismos de auditoración, control y evaluación del empleo de la interoperabilidad por los EE.MM. Las autoridades nacionales designadas para la gestión de las consultas de interoperabilidad serán responsables del tratamiento y de la calidad de los datos por las autoridades designadas, incluyendo aquellos datos que hayan sido compartidos con otros EE.MM en el marco de intercambios de información bilateral, correspondiéndoles, por tanto, la obligación de remitir periódicamente una relación estadística de las consultas realizadas por todas las autoridades designadas, tanto las competentes en materia de inmigración, fronteras y visados, como las autoridades competentes de las FCS, en aplicación de los artículos 20 y 22.

En este último caso los PACs remitirán no solo las consultas autorizadas y realizadas, sino también la efectividad de las mismas a los fines perseguidos.

Por su parte, la Comisión europea remitirá periódicamente al Parlamento europeo y al Supervisor europeo de protección de datos informes de valoración del tratamiento de datos de interoperabilidad realizados por los EEMM, así como también facilitará los registros de las consultas realizadas, en aplicación de los artículos 20 y 22, por las autoridades designadas.

Desde el punto de vista de su operatividad, las regulaciones han establecido una estructura orgánica de gobernanza compuesta por el comité de gestión del programa, denominado Consejo de administración del programa de interoperabilidad y el grupo consultivo de interoperabilidad que supervisarán, monitorizarán y rendirán cuentas del proceso de implantación. Asimismo prepararán la normativa derivada del ejercicio de la potestad reglamentaria de la Comisión en los aspectos técnicos de ambas regulaciones, a través de la adopción de cuatro actos de ejecución y dos actos delegados, a través de un comité y un grupo de expertos creados ad hoc, en aplicación de los artículos 74 del Reglamento 2019/817 y del artículo 70 del Reglamento 2019/818 para los actos de ejecución, y del artículo 73 del Reglamento 2019/817 y del artículo 69 del Reglamento 2019/818, respectivamente, con el horizonte de culminar la interoperabilidad a finales de año 2023.

La Comisión contemplaba una hoja de ruta de implantación de la interoperabilidad, que concluiría a finales de 2023, para completar el desarrollo y las comprobaciones de todos los componentes necesarios y conseguir que los sistemas de información de fronteras, migración y seguridad europeos sean interoperables. Esto no significa que inmediatamente a esa fecha los sistemas de información europeos sean ya interoperables, ni que la consecución de la interoperabilidad real en la práctica se alcance de forma inmediata a partir de esa fecha, sino que se producirá como resultado de la conclusión de los periodos de validación y pruebas técnicas a los sistemas que se vayan sucediendo, realizando, y que progresivamente irán determinando y concretando el inicio del funcionamiento de la interoperabilidad.

De esta forma, la Comisión europea remite su resultado de informes sobre los avances y preparativos para su completa implementación, incluyendo los gastos realizados y un análisis de riesgos que pueden incidir en los costes finales presupuestados del proyecto. A partir de que cada componente de la interoperabilidad entre en funcionamiento, los EE.MM notificarán a EU-LISA la lista de autoridades que podrán utilizar el PEB, el RCDI y el DIM o tener acceso a ellos (art. 71). El inicio de la interoperabilidad se producirá mediante un acto final de ejecución de la Comisión europea.

Según lo expuesto, la aplicación de los reglamentos y actos legislativos de la interoperabilidad obligará a los EE.MM a introducir notables cambios, normativos y operativos, tanto en la gestión como en la interacción con los sistemas interoperables que implicarán la adopción de nuevos procedimientos de trabajo y control de calidad de los datos, así como también la realización de inversiones, técnicas, materiales y personales, para disponer de los recursos necesarios que permitan operar en interoperabilidad con las FCS designadas de los EE.MM, que serán nuestros socios europeos en la consulta y explotación de los datos interoperables. Por ello resulta comprensible la necesidad de realizar una evaluación de impacto de la interoperabilidad a nivel nacional de nuestro país que permita anticipar la determinación de necesidades de

recursos técnicos y materiales, de formación técnica y operativa, de financiación, de dimensionamiento de estructuras administrativas de servicio a los usuarios finales que hagan posible que la implementación completa de la parte nacional de la interoperabilidad llegue a buen puerto en los plazos previstos.

Sin embargo tampoco podemos soslayar el impacto de la crisis originada por la pandemia de la COVID-19, cuyos efectos previsiblemente consistirían en la demora de los plazos establecidos para implementar la nueva arquitectura integrada de la interoperabilidad con los consiguientes sobrecostes de la implantación del proyecto. Para mitigar los riesgos asociados al proyecto en el actual contexto sanitario consideramos necesario la elaboración de un plan de contingencia, tanto europeo como nacional, que permita adoptar las decisiones que correspondan para evitar que el proyecto pueda paralizarse o sufrir retrasos considerables.

Sin lugar a dudas, esta auténtica revolución normativa de los sistemas de información europeos supone un auténtico desafío tecnológico y económico de implantación. No debemos olvidar que la financiación del mantenimiento de los sistemas de información es compartida entre los EE.MM y la Comisión Europea respecto de la infraestructura nacional de los sistemas y de arquitectura central de los mismos, respectivamente, estimándose el coste de implantación de las mejoras tecnológicas de 169,8 millones de euros a los que se añaden 28,5 millones de euros de costes de mantenimientos anuales.

#### **4. LOS PREPARATIVOS DE LA INTEROPERABILIDAD EN ESPAÑA**

Nuestro país participó en las discusiones y trabajos del Grupo de Alto Nivel constituido para elaborar las opciones de aplicación técnica y operativas de los reglamentos de interoperabilidad donde se fraguó la secuencia de las conexiones para las consultas interoperables, por lo que se estaba en condiciones de valorar el impacto del nuevo diseño de los sistemas de información europeos respecto a la arquitectura, la gestión de las consultas y el flujo de las comunicaciones nacionales derivadas de los mismos. Se presume que cada Ministerio y organismo nacional afectado han realizado análisis sectoriales en profundidad como corresponde a este tipo de proyectos, teniendo como referencia el estudio de viabilidad de la Comisión a través de EU-LISA.

Sin embargo, no ha sido hasta 2021, transcurrido un año de la aprobación de los reglamentos de la interoperabilidad, cuando se iniciaron los preparativos y se han adoptado las primeras decisiones respecto a los órganos y autoridades de control nacionales de los nuevos sistemas de información que, como hemos descrito, resultan claves para la realización de las consultas interoperables.

El impacto de la pandemia de la COVID-19 y su evolución en nuestro país en los dos últimos años ha afectado negativamente al desarrollo de los preparativos nacionales de la interoperabilidad. Las medidas iniciales a implantar en los cuerpos policiales eran las nuevas funcionalidades del SIS II de cara a la interoperabilidad (datos dactiloscópicos), como parte de la reforma del reglamento SIS II de 2019, cuya licitación y adjudicación ya se ha realizado (aunque con retraso respecto a la fecha prevista por la Comisión europea de finales de 2020). A continuación, las siguientes medidas a poner en marcha estarían referidas a los procesos de licitación y contratación de los sistemas de información europeos ex novo que formarán parte de la interoperabilidad.

Nos estamos refiriendo al SES, al SEIAV y al ECRIS-TCN. Se tiene conocimiento de que ya fue publicada la licitación del pliego de prescripciones técnicas del SES, en el portal de contratación pública de la Administración General del Estado.

Sin embargo, a estas alturas el proyecto técnico nacional de implantación del sistema de información de entradas y salidas figura todavía en la plataforma de contratación del Estado en fase de licitación, con toda la documentación desde noviembre de 2019, si bien figura como “Resuelta”, pero no adjudicada, por lo que consideramos que se habrá anulado todo el procedimiento de licitación, probablemente por desistimiento de la Administración. Desconociendo las motivaciones de la inexistencia de adjudicación, salvo que se haya replanteado el procedimiento de licitación y haya sido declarado sujeto a procedimiento negociado sin publicidad por razones, entendemos, de seguridad. Consideramos que el retraso en el proceso de contratación pública de este sistema de información, que fue objeto de comunicado de prensa<sup>3</sup> por parte del Ministerio del Interior, originará irremediablemente una demora en la fecha establecida por la Comisión Europea para la puesta en funcionamiento no solo del sistema sino de la propia interoperabilidad de los sistemas de información europeos.

Por lo que respecta a la designación de los órganos nacionales de gestión y acceso a la interoperabilidad, se tiene conocimiento que la Secretaría de Estado de Seguridad comunicó a la Comisión europea en el último trimestre del año 2020 los nombramientos y roles establecidos en los reglamentos de los sistemas interoperables. La asignación de todos los roles de autoridad respecto al SES será determinada finalmente por la Secretaría de Estado de Seguridad (lo más lógico sería que recayese en la Subdirección General de Sistemas de Información y Comunicaciones de la Secretaría de Estado de Seguridad, SGSICS), ya que así figuraría como Autoridad Nacional común para el acceso de las autoridades competentes españolas, “de inmigración”, “fronteriza” “visados” y “seguridad ciudadana”. Se tiene conocimiento que la Guardia Civil ya ha sido declarada autoridad designada para constituirse como PAC para las consultas de prevención, detección e investigación de delitos graves y terrorismo. En este sentido sería muy beneficioso disponer de algún tipo de declaración o recomendación de la Comisión proporcionando ejemplos de buenas prácticas en la designación de autoridades nacionales y los PACs, el ejercicio de control de accesos y gestión de los flujos de información, con la finalidad de homogeneizar la gestión de la interoperabilidad a nivel supranacional, “como acertadamente sostiene” (Galli, Francesca, 2019).

En este momento se considera probable que la interfaz nacional uniforme de acceso (NUI) al PSB se ubique en el Centro Tecnológico de la Seguridad, dependiente de la SGSICS, si bien según establece el PPT del EES figurarán dos NUIs, una para

---

3 Interior gastará 4,1 millones en implantar la nueva ‘frontera inteligente’. La nueva herramienta recogerá la imagen facial y cuatro huellas dactilares de los viajeros extracomunitarios que entren en el espacio Schengen. La herramienta, que deberá estar operativa en 24 meses, recogerá las fechas y lugares de entradas y salidas —además de los de denegación de entrada— de todos los ciudadanos extracomunitarios que crucen las fronteras españolas. El nuevo sistema informático de Interior se conectará al sistema de entradas y salidas (EES en sus siglas en inglés) puesto en marcha por el Consejo de Europa. A través de él, el resto de países del acuerdo Schengen podrá consultar los datos de los viajeros extracomunitarios que entren por las fronteras españolas. Por su parte, Policía Nacional y Guardia Civil también podrán revisar los “historiales de viaje” que vuelquen otros Estados. [https://elpais.com/politica/2019/12/10/actualidad/1575995791\\_087672.html](https://elpais.com/politica/2019/12/10/actualidad/1575995791_087672.html)

Ministerio del Interior y otra para el MAEC, localizándose las infraestructuras de acceso en los sistemas operativos de servicios de ambas FCSE<sup>4</sup>.

Asimismo y en lo que respecta al SEIAV, no figura en la mencionada plataforma de contratación del sector público ningún procedimiento de licitación, por lo que no se habrá ni siquiera formalizado el expediente de contratación pública previo. Lo que sí parece haberse producido es la asignación al Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) de la condición de Autoridad Nacional para el acceso de las autoridades asignadas (FCS), probablemente inducida por su vinculación operativa anterior con los datos de Registro de Nombre de Pasajeros (PNR), a través de la Unidad de Información de Pasajeros (PIU) prevista en la Directiva europea de creación del PNR (en el caso español, Oficina Nacional de Información de Pasajeros – ONIP-), con la que comparte similitudes en lo relacionado en la prevención, detección e investigación de delitos graves y terrorismo, se halla en dicho organismo. Esto es debido a que la verificación de solicitudes debe tener disponible la información necesaria contenida en las bases de datos de interés, entre ellas los ficheros de Sistema de Coordinación de Investigaciones (SCI) y al Sistema de Coordinación de Investigaciones Antiterroristas (SICOA), respectivamente, ubicados en el CITCO. Queda por determinar qué autoridades serán designadas como PACs, en quien recae la responsabilidad de monitorización y autorización de las consultas de prevención, detección e investigación de delitos graves y terrorismo de forma definitiva.

Nuestro país, en vista de lo anterior, no se encuentra en condiciones de cumplir con el plazo de operatividad real del SES previsto para abril del año 2022 en el que SES Nacional se conecte al SES Central, que incluso preveía el inicio de los test de validación en el presente año, mientras que otros países (Francia, Bélgica e Italia, entre otros). Por ello, consideramos necesario que se resuelvan las cuestiones de contratación de la implantación nacional del SES, de forma que resulte menos compleja, con las especificaciones necesarias y despojándola de cuestiones controvertidas en el momento presente, para que pueda resolverse en el menor plazo de tiempo posible. Además, sería necesaria otra licitación que contemple la instalación y adquisición del hardware y software que soporte datos biométricos del sistema de información, para todos los puestos fronterizos habilitados a enlazar, así como también establecer los convenios pertinentes con los operadores estatales encargados de la gestión de puertos y aeropuertos, esto es, Puertos del Estado y Aeropuertos Españoles y navegación aérea, (AENA), respectivamente.

Por último, no debemos olvidar que los otros dos sistemas de información europeos de nueva creación, el ECRIS-TCN, y el sistema de información de visados (VIS), cuyos procedimientos de reforma se encuentra finalizando la tramitación legislativa europea correspondiente, formarán parte de las consultas interoperables, según lo dispuesto en los Reglamentos de interoperabilidad. La transformación implícita de la interoperabilidad afectará, por tanto, no solo a los sistemas de información dependientes del Ministerio del Interior, sino también a los respectivos de los Ministerios de Justicia y Asuntos Exteriores, así como también a las servidumbres de accesos sobre los mismos autorizados a otros Ministerios para el ejercicio de sus competencias, como

4 Pliego de prescripciones técnicas para la contratación de un nuevo desarrollo de ingeniería para la implementación del nuevo sistema de registro electrónico de entradas y salidas y su conexión al sistema central del EES (proyecto Entry / Exit system, EES), p. 11.

pueden ser los Ministerios de Trabajo y Economía Social (autorizaciones de trabajo) y el de Inclusión, Seguridad Social y Migraciones (autorizaciones extranjería-residencia) o el propio Ministerio de Exteriores (consultas SIS II para la concesión de visados).

Hubiese sido más lógico, y creemos también que, ágil y efectivo, haber iniciado el proceso de implantación de la interoperabilidad de forma interdepartamental y liderado por una comisión nacional estable designada al efecto con la participación de los ministerios implicados y que contará con una evaluación de impacto y dotación presupuestaria consecuente, pues todos y cada uno de ellos, en diversa medida, se verán afectados y todo ello teniendo en cuenta el escenario macroeconómico nacional de los próximos años.

El mantenimiento del formato del HLEG, en formato de grupo convocado y reunido a demanda, hubiera sido de gran ayuda para mantener el impulso inicial y establecer un plan de acción de implementación en sintonía con la evaluación de la Comisión europea. En este sentido, la constitución del grupo de trabajo interno para apoyar los trabajos del representante nacional en el HLEG 2016-2017 tendría que haberse prolongado en el tiempo, incluso durante la tramitación europea de las normas de interoperabilidad, pues hubiera contribuido tanto a reforzar la posición institucional previa al desarrollo nacional como a determinar, de forma planificada y anticipada, las necesidades técnicas de implementación inmediata (para adaptarse a las modificaciones individuales de los reglamentos de los sistemas de información existentes), así como la provisión de recursos materiales y financieros correspondientes para la contratación pública secuencial o por lotes.

## **5. EL PROCESO DE ADAPTACIÓN DE LA GUARDIA CIVIL A LA INTEROPERABILIDAD**

La importancia estratégica de los sistemas de información y de las tecnologías de las comunicaciones en el contexto de la sociedad de la información y del conocimiento reside en la capacidad de incrementar tanto la cantidad como la calidad de los servicios ofertados por cualquier institución pública o privada. La disponibilidad y explotación de sistemas automatizados de información en la prestación del servicio público de seguridad ciudadana proporciona a los cuerpos policiales mayor eficacia, agilidad y rigor en el ejercicio de sus funciones de prevención e investigación de delitos e infracciones administrativas.

La Guardia Civil, en el ejercicio del amplio elenco de funciones policiales asignadas en el ordenamiento jurídico del Estado viene siendo plenamente consciente de la necesidad permanente de avanzar en la modernización y actualización tecnológica de sus sistemas informáticos y, en particular, aquellos que dan soporte a la prestación del servicio al ciudadano, esto es los sistemas de información policial para la seguridad. Los sucesivos Planes estratégicos plurianuales del Cuerpo contienen ejes de actuación relacionados con la mejora de las capacidades de los sistemas de información e inteligencia del Cuerpo a través de la integración de las diversas plataformas de sistemas de información en el sistema integrado de gestión operativa del cuerpo.

En el sistema SIGO se hallan integrados, conforme la normativa nacional de seguridad de sistemas de información, los accesos, directa o indirectamente consumibles, a los sistemas de información europeos instituidos en aplicación del Derecho

europeo. Si bien hasta la fecha solo resulta directamente consumible el SIS II, es de esperar que suceda lo mismo con los sistemas de información interoperables. Lo cierto es que, desde la aprobación de los Reglamentos europeos de reforma del SIS II y de los correspondientes del SES y SEIAV, resulta oportuno y pertinente abordar la necesidad de propiciar un proceso nacional de implantación de la interoperabilidad objetivo y equilibrado, que satisfaga por igual las necesidades operativas y de servicio de los cuerpos policiales de nuestro país para aprovechar las nuevas capacidades de información europeas y su aplicación a la seguridad pública y estar en condiciones de mejorar incluso el servicio a nuestros ciudadanos en todos los rincones de nuestra geografía, particularmente en la España vaciada. Máxime si tenemos en cuenta el potencial actual, 77.000 efectivos y más de 2.250 unidades, tanto de seguridad ciudadana como de especialidades, y 1.963 puestos en las 50 provincias y en las ciudades autónomas de Ceuta y Melilla, con cometidos de seguridad ciudadana en casi 6800 municipios y, además, ostentando la condición de Autoridad de Coordinación frente a la inmigración irregular en el Estrecho y en Canarias<sup>5</sup>.

Dada la dimensión transnacional de la interoperabilidad, la Guardia Civil dispone de las capacidades, conocimiento y experiencia necesarias para hacer frente a un desafío de estas proporciones, como lo es la conexión a los sistemas interoperables europeos. Por ello, consideramos pertinente la presentación de cuantos proyectos técnicos sean necesarios para que las distintas unidades de la Guardia civil puedan consumir directa, desasistida y automatizadamente la información interoperable europea. Asimismo, deberá asegurarse en los próximos años de recibir y disponer de crédito presupuestario para acometer las modificaciones técnicas derivadas en las plataformas corporativas del Cuerpo, en la parte financiera no asumida por el presupuesto comunitario.

## BIBLIOGRAFÍA

CARRERA, Sergio; MITSILEGAS, Valsamis (eds), *Constitutionalising the Security Union : effectiveness, rule of law and rights in countering terrorism and crime*, Brussels : CEPS, 2017, 65-72, <https://www.ceps.eu/publications/constitutionalising-security-union-effectiveness-rule-law-and-rights-countering>

DÓCZI, ZOLTÁN, “The Development, the Integration and the Assessment of the Existing Large-Scale IT Systems in the Area of Freedom, Security and Justice”, *Acta juridica hungarica* 54, No 2, pp. 164–183 (2013).

Illamola Dausà, Mariona, “EU-LISA, el nuevo modelo de gestión operativa de las distintas bases de datos de la UE EU-LISA, the new model of operational management of the various EU databases” *Revista CIDOB d’Afers Internacionals*, n.111, p. 105-126, [www.cidob.org](http://www.cidob.org), Consultado el 13 de marzo de 2021.

Galli, Francesca, “Interoperable Law Enforcement Cooperation Challenges in the EU Area of Freedom, Security and Justice”, Working Paper, EUI RSCAS 2019/15 Robert Schuman Centre for Advanced Studies, <http://hdl.handle.net/1814/61045>, p.10.

5 Comparecencia de la directora general de la Guardia Civil, COMISIONES, Año 2021 XIV LEGISLATURA Núm. 327, INTERIOR, Comisiones, núm. 327, de 18/03/2021, Sesión núm. 12, el 18 de marzo de 2021, Diario de sesiones del Congreso de los Diputados.

Tomaszycki, Krzysztof, “La interoperabilidad de los sistemas de información europeos de fronteras y gestión de la migración para mejorar la seguridad” *facta universitatis Series: Law and Politics* Vol. 16, No 3, 2018, Original Scientific Paper, Faculty of Law, University of Bialystok, Poland.pp. 195-211, p.205, <https://doi.org/10.22190/FULP1803195T>.

Blasi Casagran, Cristina, “Implicaciones de los Derechos Fundamentales de la Interconexión de las bases de datos de migración y policiales en la UE”, *Human Rights Law Review*, 2021, Oxford University Press, 00, 1–25 doi: 10.1093/hrlr/ngaa057, consultado el 28 de abril de 2021.

Jokhadze, Nata, “La implementación de la interoperabilidad de los sistemas de información europeos en el ámbito de Justicia y asuntos de interior. Desafíos y Oportunidades” Facultad de Tecnología de la Universidad de Tallin, Escuela de negocios y gobernanza Ragnar Nurkse Departamento de innovación y gobernanza (RND) Tesis del programa de gobernanza tecnológica y transformación digital, Tallin 2020.

Aden, Harmut, “Interoperabilidad entre las bases de datos europeas de policía y de migración: Riesgos para la Privacidad”, *Revista de Derecho Público Europeo*, Vol 1, 2020.

Brouwer, Evelin, “Bases de Datos de gran escala e Interoperabilidad en las políticas de migración y Frontera: Una aproximación no discriminatoria a la retención de datos”, *Revista Europea de Derecho*, Vol 1, 2020.

Curtin, Diandre y Bastos, Felipe Brito, “La Compartición de Información Interoperable y las cinco innovadoras fronteras de gobernanza de la Unión: Un asunto especial”. *Revista de Derecho Público Europeo*, nº 1, 2020.

Reglamento (UE) 1077/2011 del Parlamento Europeo y del Consejo de 25 de octubre de 2011 por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia. DOCE 1.11.2011, L 286/1, modificado por el Reglamento (UE) 1726/2018.

Reglamento 2017/2016, sobre el Sistema de Entrada y Salida (EES), “inmigración, control de fronteras, y visados” (artículo 9.2, 26 y 27) y prevención, detección e investigación de delitos graves y terrorismo” (artículos 9.3, 29 y ss.)

Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo DO L 135 de 24.5.2016, p. 53/114.

Reglamento UE 2019/816 de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los EE.MM que poseen información sobre condenas de nacionales de terceros países y apátridas a fin de complementar el Sistema Europeo de Información de Antecedentes Penales, y por el que se modifica el Reglamento (UE) 2018/1726.

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.o 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, 22.5.2019 ES Diario Oficial de la Unión Europea L 135/27.

Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816, 22.5.2019 ES Diario Oficial de la Unión Europea L 135/85.

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

Propuesta de Decisión Marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (presentada por la Comisión) {SEC(2005) 1270} Bruselas, 12.10.2005 COM(2005) 490 final 2005/0207 (CNS).

Comunicación de la Comisión al Consejo y al Parlamento Europeo, Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia. Bruselas, 10.5.2005 COM (2005) 184 final.

Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre una mayor eficacia, interoperabilidad y sinergia entre las bases de datos europeas en el ámbito de la Justicia y los Asuntos de Interior, COM(2005) 597 final, Bruselas, 24 de noviembre de 2005.

Comunicación de la Comisión europea al Consejo y al Parlamento europeo «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad», COM (2016) 205 final, de 6 de abril de 2016.

Decisión de la Comisión de 17.06.2016 por la que se establece el Grupo de Expertos de Alto Nivel (HLEG), acrónimo en inglés de High Level Expert Group) sobre los sistemas de información y la interoperabilidad, COM (2016)3780 final.

Hoja de ruta de 6 de junio de 2016 para mejorar el intercambio y la gestión de la información, con inclusión de soluciones de interoperabilidad en el ámbito de la Justicia y los Asuntos de Interior (9368/1/16 REV 1).

Conclusiones del Consejo JAI de 18 de diciembre de 2015, Reunión del Consejo Europeo (17 y 18 de diciembre de 2015), EUCO 28/15 CO EUR 13 CONCL 5.

Informe de la Comisión al Parlamento Europeo y al Consejo relativo a la situación de los preparativos para la plena aplicación de los Reglamentos de interoperabilidad con arreglo al artículo 78, apartado 5, del Reglamento (UE) 2019/817 y el artículo 74, apartado 5, del Reglamento (UE) 2019/818 de 21 de agosto de 2020, p.2.

Doc. Consejo 9028/20, IXIM 64, JAI 514, COMIX 273 Reevaluación cronológica hacia la implementación de la arquitectura de interoperabilidad JAI”, de 3 de julio de 2020, p.2.

Documento de Trabajo de la Comisión Europea, resumen ejecutivo de evaluación de impacto, document de acompañamiento de la Propuesta de Reglamento del Parlamento Europeo y del Consejo Propuesta de Reglamento (UE) 2019/817 por el que se establece un marco para la interoperabilidad de los sistemas de información de la Unión Europea en el ámbito de las fronteras y los visados y modificación de la Decisión del Consejo 2004/512/CE, Reglamento (CE) No 767/2008, Decisión del Consejo 2008/633/JAI, Reglamento (UE) 2016/399 y Reglamento (UE) 2017/2226 y Propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establece un marco para la interoperabilidad de los sistemas de información de la Unión Europea en el ámbito de la cooperación judicial, el asilo y la migración , Strasbourg, 12.12.2017, SWD(2017) 474 final.

Informe del grupo ad hoc para el estudio de los sistemas de información del tercer pilar, doc. Consejo 8857/03 LIMTIE JAI 118, de 6 de mayo de 2003, p.5.

Comentarios del Supervisor Europeo de Protección de Datos a la Comunicación de la Comisión sobre la interoperabilidad de las bases de datos europeas (2006) de 10 de marzo de 2006. [https://edps.europa.eu/sites/edp/files/publication/06-03-10\\_interoperability\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/06-03-10_interoperability_en.pdf)

Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. publicado en: «BOE» núm. 272, de 09/11/2017. Entrada en vigor: 09/03/2018.

RD\_L 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y LO 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales.

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. Jefatura del Estado «BOE» núm. 77, de 31 de marzo de 2015 Referencia: BOE-A-2015-3442.