

La protección de datos en la cooperación policial transfronteriza

Selena
Cebrián Beltrán

Doctora por la Universidad de Valencia

SUMARIO:

- I. Introducción
- II. Los instrumentos de cooperación policial y su protección de datos
- III. Las diferencias en el tratamiento de datos de las víctimas del delito y del sospechoso
- IV. Consideraciones finales y recomendaciones

FICHA DE LA TESIS

- **Fecha y lugar de defensa:** 17 de enero de 2025 (Universidad de Valencia)
- **Miembros del tribunal:** M^a José Ridaura Martínez (Universidad de Valencia), M^a Luz Martínez Alarcón (Universidad de Castilla-La Mancha) y Francisco Javier Donaire Villa (Universidad Carlos III de Madrid).
- **Director y/tutor:** Luis Jimena Quesada y Beatriz Tomás Mallén.
- **Mención internacional:** No
- **Libro:** Selena Cebrián Beltrán (2025). *La protección de datos en el contexto de la cooperación transfronteriza de las autoridades policiales*. Tirant lo Blanch
<https://editorial.tirant.com/es/libro/la-proteccion-de-datos-en-el-contexto-de-la-cooperacion-transfronteriza-de-las-autoridades-policiales-selena-cebrian-beltran-9788410957039>

NOTA BIOGRÁFICA:

Selena Cebrián Beltrán es graduada en Derecho y Ciencias Políticas y de la Administración Pública (2016) por la Universidad de Valencia donde también obtuvo el Máster de Acceso a la Abogacía (2020). También ha realizado un Máster en Compliance y Protección de Datos (2022) por la Universidad de Málaga. Es doctora cum laude por la Universidad de Valencia. Actualmente es profesora sustituta de Derecho Administrativo en la Universidad de Valencia y en la Universidad Jaume I de Castellón y profesora de Derecho Constitucional en la Universidad Isabel I. Forma parte de los grupos de investigación “Del actual aislamiento hacia una necesaria cooperación entre Autoridades de supervisión y control en la aplicación de la legislación digital” (CONECTA).

ESTADO DE LA CUESTIÓN DEL TEMA TRATADO:

La globalización del delito exige una cooperación policial multinivel basada en el intercambio de datos. Para ello, existen numerosos instrumentos en la Unión Europea y en el ámbito internacional que regulan las garantías sobre las que debe

operar esta transmisión, especialmente la protección de datos. A ello se suma la aparición de nuevas tecnologías que, si bien mejoran la eficacia de la seguridad pública, plantean riesgos para los derechos fundamentales. Esta tesis pretende determinar si la normativa vigente proporciona un nivel adecuado y uniforme de protección de los datos personales, analizar las distintas condiciones que rigen su tratamiento según la posición del interesado —principalmente víctimas y sospechosos—, identificar los aspectos susceptibles de mejora y proponer medidas para reforzar las garantías aplicables.

PALABRAS CLAVE:

Protección de datos, cooperación policial, Inteligencia Artificial, seguridad pública.

KEYWORDS:

Data protection, police cooperation, Artificial Intelligence, public safety.

I. INTRODUCCIÓN

Hay tesis que surgen como una continuación natural de los estudios universitarios; otras, como esta, son fruto de la experiencia acumulada en la trayectoria profesional. Tras finalizar el doble grado en Derecho y Ciencias Políticas, comencé a preparar las oposiciones para la escala ejecutiva de la Policía Nacional en el año 2017. Aunque no superar la fase de entrevista y diversas circunstancias personales me llevaron a buscar otras salidas profesionales, el azar no tardaría en vincularme de nuevo con este ámbito. Meses más tarde, inicié mi andadura profesional en la misma academia donde me había formado, institución con la que permanecí vinculada durante más de siete años. Fue allí donde comencé a impartir clases y descubrí mi verdadera vocación y pasión por la docencia.

Durante estos años, casi por casualidad, se cruzó en mi camino un Máster de Protección de Datos y *Compliance* y, a través de él, me adentré en la interesante y compleja aventura de la protección de datos.

La tesis en la que se fundamenta este trabajo nace de la confluencia entre la práctica policial diaria y la complejidad de su marco regulatorio: una miríada de textos legales, bases de datos e iniciativas de cooperación transfronteriza, así como las normativas de protección de datos aplicables a cada uno de ellos. Asimismo, este proyecto es el resultado del privilegio de haber sido acogida como discípula por mis directores de tesis, los catedráticos Dr. Luis Jimena Quesada y Dra. Beatriz Tomás Mallén, quienes me demostraron que la excelencia profesional no es casualidad, sino el fruto de la pasión por el trabajo y el compromiso con la formación de las futuras generaciones.

El objeto central de esta investigación surge de reflexionar sobre una necesidad intrínseca de las autoridades encargadas del cumplimiento de la ley: la obtención y el tratamiento de datos personales durante sus actuaciones. No obstante, la labor policial diaria revela escenarios donde los instrumentos internos resultan insuficientes, haciendo imprescindible recurrir a bases de datos, sistemas de cooperación, agencias y organismos, tanto de la Unión Europea como del ámbito internacional.

Existen numerosos instrumentos de colaboración policial cuyo funcionamiento requiere la salvaguarda de diversas garantías, especialmente la protección de datos personales. Por ello, constituye un pilar esencial de esta tesis el estudio de bases de datos como el SIS, VIS, Eurodac, SES, SEIAV, ECRIS y ECRIS-TCN; de agencias y organismos como Europol, Frontex o Interpol; de iniciativas específicas como el PNR; y de instrumentos facilitadores de la cooperación como el Reglamento 2019/818 y el Reglamento Prüm II.

Tras delimitar estos instrumentos, resultaba obligado abordar el régimen de protección de datos aplicable a cada uno de ellos. Si bien en la Unión Europea este marco está articulado principalmente por la Directiva (UE) 2016/680 —con

la excepción de Europol—, el resto de las iniciativas cuenta con una normativa específica propia. No obstante, con el propósito de evitar un enfoque puramente descriptivo de las normas y la jurisprudencia, esta tesis aporta una perspectiva novedosa al explorar la aplicación del derecho fundamental a la protección de datos desde tres vertientes distintas: víctima, la persona investigada, encausada o condenada y agentes policiales.

A continuación, se sintetizarán los elementos centrales de este trabajo. En primer lugar, la diversidad de instrumentos de cooperación policial y la protección de datos aplicables a cada uno de ellos. En segundo lugar, la explicación de las diferencias existentes en la protección de datos de las víctimas y de las personas presunta y comprobadamente involucradas en un hecho criminal y el ejercicio de los derechos de acceso, rectificación, supresión y limitación del tratamiento. Finalmente, se aportará un análisis crítico de los límites de la utilización de las nuevas tecnologías de la información y la comunicación (NTIC) para la garantía de la seguridad pública.

II. LOS INSTRUMENTOS DE COOPERACIÓN POLICIAL Y SU PROTECCIÓN DE DATOS

La cooperación policial constituye uno de los pilares esenciales para salvaguardar la seguridad pública y combatir la delincuencia en un escenario caracterizado por la creciente movilidad transnacional, la globalización de las amenazas y el avance de las NTIC. Por este motivo, se ha configurado un complejo entramado de bases de datos, agencias y organismos que, bajo la perspectiva multinivel de un ordenamiento jurídico como el español, operan en dos planos principales: el intracomunitario y el internacional.

En este contexto, la protección de datos se erige como un límite esencial a la labor de las autoridades encargadas del cumplimiento de la ley. Dentro de la Unión Europea, coexisten una serie de bases de datos que permiten el acceso e intercambio de la información necesaria para la persecución de las formas más graves de delincuencia.

El Sistema de Información Schengen (SIS) es una base de datos creada en el marco del espacio Schengen para el control del cruce de las fronteras interiores por ciudadanos extranjeros. No obstante, permite apoyar a las autoridades responsables de la prevención, detección, investigación o enjuiciamiento de infracciones penales o ejecución de sanciones penales con el intercambio de información sobre personas buscadas, objetos y otras alertas relevantes para la seguridad (arts. 20, 26, 32, 36, 38, 43, 44 y 48 del Reglamento (UE) 2018/1862).

El Sistema de Información de Visados (VIS) optimiza la aplicación de la política común de visados, pero también contribuye a la prevención de amenazas contra la seguridad interior de los Estados miembros (arts. 3 y 31 Reglamento (CE) n.º

767/2008). Asimismo, Eurodac almacena huellas dactilares e imágenes faciales de los solicitantes de asilo y migrantes irregulares. Las autoridades policiales de los Estados miembros pueden acceder a estos datos para prevenir, detectar o investigar delitos de terrorismo u otros delitos graves (arts. 3, 5, 7 y 19 Reglamento (UE) 2024/1358).

El Sistema Europeo de Información de Antecedentes Penales (ECRIS) facilita el intercambio de información de los registros de antecedentes penales nacionales entre las autoridades centrales de los Estados miembros (arts. 6, 7, 8, 9 y 11 bis, Directiva (UE) 2019/884). De este sistema deriva ECRIS-TCN que extiende esta cooperación a los antecedentes de nacionales de terceros países o apátridas.

Finalmente, la próxima entrada en funcionamiento del Sistema Europeo de Entradas (SES) y el Sistema Europeo de Información y Autorización de Viajes (SEIAV) automatizará el registro de nacionales de países no miembros de la UE que ingresen al espacio Schengen y establecerá nuevas obligaciones de información para viajeros exentos de la obtención de visado de corta duración, coadyuvando igualmente a la prevención e investigación del terrorismo y la delincuencia grave.

Todos estos sistemas comparten como marco fundamental de protección de datos la Directiva 2016/680, eje sobre el cual se articulan las normativas internas de los países miembros de la UE. Dicha Directiva es el resultado de una evolución normativa iniciada por el Consejo de Europa a través del Convenio 108 (1981)¹ y consolidada en 1985 con la Recomendación N.º R (87), dirigida a regular el uso de datos personales en el sector policial.

Estos textos marcaron la senda posteriormente seguida en la Unión Europea con la Directiva 95/46/CE y la Decisión marco 2008/977/JAI del Consejo. Tras el Tratado de Lisboa, la Directiva 2016/680 busca consolidar un marco común aplicable a las particularidades del tratamiento de datos en el ámbito policial. Entre sus principales salvaguardas se encuentran: la definición de principios generales de obligado cumplimiento para el tratamiento de datos (art. 4); la posibilidad de utilizar los datos penales para finalidades distintas, pero compatibles (art. 9); la limitación del plazo de conservación de los datos personales (art. 5); la delimitación de las categorías de interesados (art. 9); el deber de informar a los interesados sobre la posibilidad de ejercer sus derechos de acceso, rectificación, supresión y limitación del tratamiento (arts. 12 – 18); la regulación de la transferencia de datos personales a terceros países u organizaciones internacionales bajo estrictas condiciones (art. 35 – 40); y la adopción de medidas técnicas para proteger la integridad de los datos personales frente amenazas internas y externas (art. 29 – 31).

1. El Convenio 108 ha sido actualizado a través de Convenio 108+ de 18 de mayo de 2018 para adaptación a los cambios surgidos para la aplicación de las NTIC.

La Directiva fue traspuesta en España por la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (en adelante, LO 7/2021)².

No obstante, cada instrumento presenta particularidades específicas, principalmente en el periodo de conservación de los datos y en la posibilidad de prohibir el intercambio de datos con otros organismos, salvo excepciones. Adicionalmente, se evidencian ciertas divergencias fruto de la propia naturaleza de la Directiva, puesto que durante su trasposición al ordenamiento jurídico de los Estados miembros de la Unión Europea se han producido desajustes, problemas de interpretación o falta de definición de algunos elementos.

Estas discrepancias interpretativas han motivado diversos pronunciamientos por parte del Tribunal de Justicia de la Unión Europea (TJUE). En ellas destacan la STJUE (Gran Sala) de 22 de junio de 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19 sobre el ámbito de aplicación de la Directiva; la STJUE (Sala 5ª) de 24 de febrero de 2022, *SS SIA c. Valsts ieņēmumu dienests*, C-175/20, sobre la definición de autoridad competente; y la STJUE (Gran Sala) de 2 de octubre de 2018, *cuestión prejudicial de la Audiencia Provincial de Tarragona*, C-207/16, sobre la definición de delito grave.

Conviene destacar que, aunque el VIS, Eurodac, SES y SEIAV fueron concebidas inicialmente para el control de las fronteras, sus funcionalidades se han ampliado progresivamente hacia el ámbito de la persecución penal. Este fenómeno traza una correlación entre la condición de migrante y la articulación de un control reforzado basado en su potencial vinculación con el crimen.

En cuanto a las agencias de cooperación, Europol destaca como actor principal para fomentar la prevención y la lucha contra las formas graves de delincuencia y terrorismo que afecten a dos o más Estados miembros. Si bien Europol queda excluido del ámbito de aplicación de la Directiva 2016/680, su Reglamento incorpora un régimen particular cuyas garantías son sustancialmente similares a las de dicha norma.

En el plano internacional, la cooperación policial se canaliza fundamentalmente a través de dos instrumentos: Interpol y la iniciativa PNR. El PNR articula el tratamiento de los datos de reserva de vuelos con origen o destino en la Unión Europea con fines de prevención penal, quedando sometido al marco de la Directiva 2016/680 (arts. 1, 3 y 10 y Considerando 15 Directiva 2016/681). Más allá

2. Este retraso en la transposición motivó la STJUE (Sala Octava) de 25 de febrero de 2021 (*Comisión contra España*, asunto C-658/19), un fallo histórico en el que el Tribunal impuso, por primera vez, de forma simultánea, una suma a tanto alzado y una multa coercitiva diaria.

de las fronteras comunitarias, estos datos son objeto de intercambio con Estados Unidos, Canadá o Australia al amparo de los acuerdos de colaboración adoptados.

Interpol centraliza la cooperación de 196 países miembros a través de una red global de intercambio de información regulada por su Reglamento de Tratamiento de Datos (en adelante, RITD). Este texto incluye los principios fundamentales para la protección de datos como exactitud, transparencia, confidencialidad o seguridad de la información; regula el ejercicio de los derechos de acceso, rectificación o eliminación de los interesados (art. 18); limita la conservación de los datos almacenados (art. 49); e incluye un catálogo de obligaciones para los participantes (arts. 2, 3, 35).

Todo ello evidencia la notable complejidad del sistema de intercambio de información, la coexistencia de diversos regímenes de protección de datos y las asimetrías surgidas en los ordenamientos jurídicos internos de los Estados miembros a raíz del proceso de trasposición. Por esta razón, en los últimos años han visto la luz herramientas orientadas a facilitar dicha colaboración.

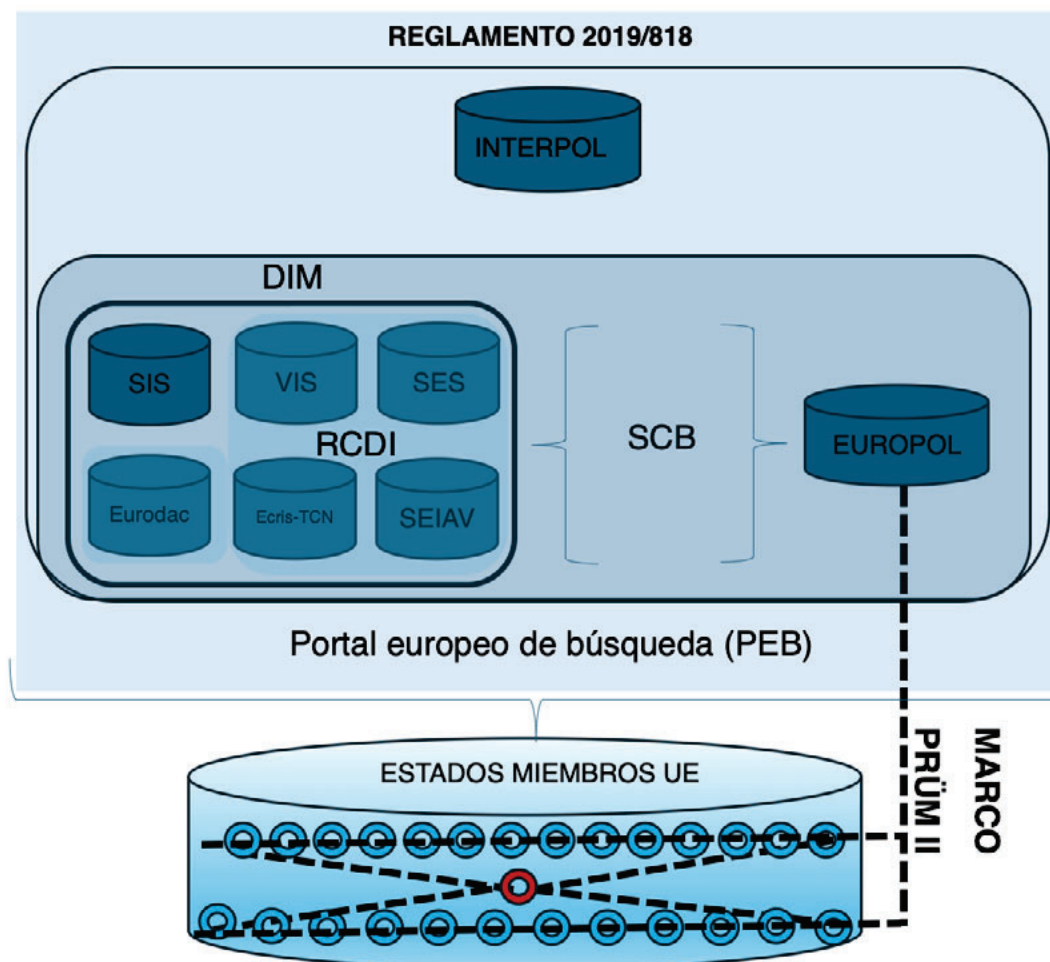
El Reglamento 2024/982 establece el marco Prüm II diseñado para agilizar el intercambio de información penal y de datos de matriculación de vehículos entre las autoridades competentes de los Estados miembros, así como entre estos y Europol, a efectos de la prevención, detección e investigación de infracciones penales. Todos estos intercambios de información quedan sujetos a la Directiva 2016/680, el Reglamento 2018/1725, el Reglamento Europol y el Reglamento General de Protección de Datos.

El otro instrumento indispensable para lograr esta interoperabilidad es el Reglamento 2019/818, que entró en vigor el 12 de junio de 2026. Su arquitectura se compone de:

- Portal Europeo de Búsqueda (PEB), que permite el acceso rápido, ininterrumpido e inmediato de las autoridades de los Estados miembros y de las agencias de la UE a los sistemas de información de la UE (SES, VIS, SEIAV, SIS, Eurodac y ECRIS-TCN), Europol y a las bases de datos de Interpol.
- Correspondencia Biométrica Compartida (SCB compartido), que almacenará plantillas biométricas obtenidas a partir de los datos del RCDI y el SIS, permitiendo la consulta de datos biométricos a través de varios sistemas de información de la UE.
- Registro común de datos de identidad (RCDI), que contiene un archivo individual de cada persona registrada al menos en una de las bases de datos, con el objetivo de garantizar una identificación exacta de cada individuo.
- Detector de identidades múltiples (DIM), que apoya el funcionamiento del RCDI y facilita la detección de personas registradas con dos identidades diferentes.

La arquitectura diseñada por el Reglamento 2019/818 simplifica la búsqueda de información de las autoridades de cumplimiento de la ley y posibilita la garantía del principio de exactitud, uno de los más relevantes durante las investigaciones policiales. El principio de exactitud no solo exige la veracidad de la información, sino también su constante actualización. Una identificación errónea del sujeto activo o pasivo de un hecho criminal o de su edad, puede repercutir en el éxito de la tarea policial transnacional.

Funcionamiento gráfico del Reglamento 2019/818 y del Reglamento Prüm (marco Prüm II)



Fuente: Elaboración propia

III. LAS DIFERENCIAS EN EL TRATAMIENTO DE DATOS DE LAS VÍCTIMAS DEL DELITO Y DEL SOSPECHOSO

La identificación de las partes implicadas en un hecho delictivo es una tarea compleja, especialmente en las fases iniciales de una investigación penal, cuando la información disponible suele ser limitada y susceptible de modificación a medida que avanzan las actuaciones policiales.

Los distintos instrumentos de cooperación policial de la UE regulan los supuestos y condiciones en los que pueden intercambiarse datos personales. Sin embargo, existen algunas diferencias en el tratamiento de los datos de las víctimas del delito y los datos de las personas sospechosas o condenadas.

La Directiva 2016/680 y la ley de trasposición española, la LO 7/2021, distinguen diferentes categorías de interesados cuyos datos son objeto de tratamiento por las autoridades competentes. Asimismo, el Reglamento de Europol y el RITD también tratan estos roles.

De este modo, la configuración de la parte activa del delito se articula en torno a las siguientes categorías y matices normativos³:

1. Sospechosos: personas sobre las que existen motivos fundados para presumir que han cometido o que podrían cometer un delito. La LO 7/2021 y el Reglamento de Europol añaden a los anteriores a los colaboradores del delito. Para Interpol, solo será sospechoso quien, en el marco de una investigación policial, es considerado el posible autor del crimen, pero que todavía no es objeto de la acción penal.
2. Personas objeto de una acción penal o acusados: esta situación de imputación solo está prevista en el RITD.
3. Personas condenadas o sancionadas por una infracción penal: personas enjuiciadas sobre las que haya recaído sentencia condenatoria. A efectos de Interpol serán denominados “convictos”.
4. Terceros involucrados en la infracción penal, entre los que se incluyen las personas de contacto de los sospechosos y de los condenados.

En la parte pasiva del delito se encuentra la víctima. En el ámbito internacional, su definición es un asunto complejo, ya que no se dispone de un concepto universal. Particularmente, en la ONU su caracterización depende del delito cometido

3. Clasificación extraída del art. 6 de la Directiva 2016/680; art. 9 LO 7/2021; art. 44 del RITD y Anexo II del Reglamento de Europol.

contra ellas⁴. A este déficit de uniformidad ha contribuido la ausencia de consenso en torno a una definición común de terrorismo.

Interpol opta por una vía más práctica e indica que la víctima es la persona que ha sido objeto de un delito.

Inicialmente el Consejo de Europa adoptó una definición restrictiva circunscrita únicamente a las personas que hubieran sufrido delitos violentos. Posteriormente la Recomendación Rec (2006) 8 sobre asistencia a las víctimas amplió formalmente el concepto para dar cobertura a las víctimas de cualquier tipo de delito y a sus familiares.

La Directiva 2011/29 de la UE consolidó una definición integral de víctima, aplicable solo a personas físicas. Además, consolidó la tendencia de normas anteriores al extender formalmente la condición y protección de “víctima indirecta” a los familiares y dependientes de la víctima directa.

La categorización como víctima entra en conflicto, en no pocas ocasiones, con la condición de testigo. De hecho, en la legislación española, si la víctima decide no personarse en el procedimiento penal puede ser llamada en calidad de testigo, quedando sujeta a las obligaciones legales de esta figura.

Sentadas las bases anteriores, resulta de especial interés examinar las diferencias concretas en el tratamiento de datos personales que prevén los distintos instrumentos de cooperación policial.

El Reglamento SIS considera a la víctima como el objeto de protección del sistema (art. 32) y establece condiciones específicas para poder incluir datos personales biométricos identificativos (art. 42 y 43). Los datos del sospechoso pueden ser consultados de manera activa a través de impresiones dactilares o palmares del lugar del crimen.

El Reglamento Eurodac permite el acceso a sus datos con fines de identificación exacta de la víctima y del sospechoso (Considerando 13 y 21).

El Reglamento Europol es más concreto al señalar que la protección de víctimas, testigos, personas con información relevante y menores resulta crucial. Para estos colectivos, los datos personales tratados serán los comunes y se limitarán a lo estrictamente necesario; si se requiere el uso de información sensible, esta solo podrá tener carácter complementario respecto de los datos principales

4. Declaración de los principios fundamentales de justicia relativos a las víctimas del delito y a las víctimas del abuso de poder (1985), Principios y directrices básicos sobre el derecho de las víctimas de violaciones manifiestas (2005), Convención internacional para la protección de todas las personas contra las desapariciones forzadas (2006).

(Considerando 43). El acceso a esta información deberá contar con autorización del director ejecutivo de Europol.

Por el contrario, en lo que respecta al sospechoso, el Reglamento permite el tratamiento de información con el fin de efectuar controles cruzados, orientados a identificar conexiones o relaciones relevantes para la investigación.

El Reglamento Prüm II facilita la localización de víctimas y personas desaparecidas mediante la consulta e intercambio de datos de ADN, datos dactiloscópicos e imágenes faciales. Asimismo, en el caso de los sospechosos, permite agilizar su identificación y localización a través de la solicitud e intercambio de dicha información. El RIA permite el uso de sistemas de identificación biométrica remota para la localización e identificación de determinados sospechosos y víctimas (art. 5 y 26).

Finalmente, el RITD indica que los datos de las víctimas, testigos o menores solo podrán ser registrados para los hechos en los que tengan tal condición y se deberá especificar la finalidad del registro (art. 38). Los datos de los sujetos activos del crimen se escindirán en tres categorías, según el momento procesal en el que se encuentre la causa: sospechoso, convicto y acusado. Sobre ellos, las Oficinas centrales nacionales o internacionales pueden formular una alerta de cooperación internacional (art. 83).

A este respecto, existe un tratamiento más garantista sobre los datos de las víctimas que sobre los datos de las personas presunta y comprobadamente implicadas en una infracción penal, lo que se justifica en los siguientes motivos:

1. El tratamiento de los datos de la víctima es inevitable para investigar o enjuiciar las acciones penales.
2. Los datos de la víctima son indispensables para la aplicación de las medidas de protección oportunas que la amparen en el ámbito nacional y en el internacional, por ejemplo, mediante la Orden Europea de Protección.
3. La divulgación de los datos de la víctima acarrea consecuencias más graves que la difusión de los datos del sospechoso o condenado. Esto se debe no solo a la vulneración de su derecho fundamental a la intimidad y a la protección de datos, sino también a que su identificación pública afecta a su vida cotidiana (STEDH, (Sección 10ª), *Khelili c. Suiza*, 18 de octubre de 2011) y aumenta exponencialmente los efectos de la revictimización. Pero también la facilitación de su localización podría poner en riesgo su integridad física a manos de su agresor.
4. La persecución del crimen es uno de los objetivos primordiales de todo Estado en aras del mantenimiento de la seguridad pública y la paz ciudadana. La cooperación policial y el intercambio internacional de datos personales son fundamentales para perseguir el delito y ejecutar sentencias. Aunque el tratamiento de información del sospechoso o condenado está sujeto a salvaguardas, se prioriza de forma amplia bajo el principio del bien superior de la seguridad ciudadana, pública o nacional.

Esta prioridad de la seguridad no implica una desprotección absoluta de los derechos del sospechoso, ya que la presunción de inocencia debe ser mantenida en todo momento desde el inicio de la maquinaria de la cooperación policial (por ejemplo, STEDH (Sección 5ª), *Batiashvili c. Georgia*, 10 de octubre de 2019), hasta la existencia de una sentencia firme.

5. La especial vulnerabilidad de la víctima exige una tutela diferenciada frente a la publicación de información, tanto en el ámbito judicial como en los medios de comunicación. La difusión de la identidad no consentida de la víctima constituye una transgresión a su derecho a la intimidad (por ejemplo, en la STC 127/2003, de 30 de julio), especialmente si se trata de víctimas menores de edad.

Sin embargo y a efecto de satisfacer el interés por la prevención general, el tiempo no elimina la huella de las infracciones penales cometidas y sentenciadas, incluso después de que el individuo haya cumplido su condena, ya que estos datos cumplen un propósito social superior, tal y como muestran la STEDH (Sección 5ª), *M. L. y W. W. c. Alemania*, de 28 de junio de 2018, la STC 58/2018 de 4 de junio de 2018 y la Sentencia de la Audiencia Nacional (Sala de lo contencioso, Sección 1ª), n.º1211/2024 (n.º recurso 2301/2021), 6 de febrero de 2024.

En otro orden de cosas, el interesado puede ejercer sus derechos de acceso, rectificación, supresión o limitación sobre el tratamiento de sus datos en sistemas como el SIS, VIS, Eurodac, ECRIS-TCN, SES y SEIAV conforme a lo establecido en los arts. 12-17 de la Directiva 2016/680. Si el interesado efectúa esta acción frente a Europol podrá ejercer el derecho de acceso, rectificación, cancelación y restricción en base a los arts. 31 a 33 de su Reglamento. Interpol permite la solicitud del acceso, rectificación y eliminación de los datos tratados en su Sistema de Información (art. 18 RITD).

Sin embargo, con frecuencia este reconocimiento se da únicamente *de iure*, pero no *de facto*. Para poder ejercer estos derechos, es indispensable que el afectado tenga conocimiento de que sus datos están siendo tratados con fines penales. Esto resulta prácticamente imposible si las indagaciones previas no derivan finalmente en un procedimiento judicial.

Suponiendo que el sujeto sea consciente de la existencia de una investigación, para percatarse, por ejemplo, de la inexactitud, desactualización o la conservación excesiva de sus datos personales, es indispensable que solicite primeramente el derecho de acceso. De este modo, el derecho de acceso se erige como antesala para el ejercicio del resto de derechos.

La tercera problemática vinculada al ejercicio de estos derechos radica en la dificultad de identificar ante qué autoridad nacional o internacional se debe presentar la solicitud. España actúa como mediador en el ejercicio de los derechos de rectificación y supresión a través de la Oficina Sirene respecto de los datos contenidos en el SIS y a través del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación por los datos del VIS.

No obstante, resulta evidente que el ejercicio de estos derechos presenta una complejidad añadida cuando el caso trasciende las fronteras nacionales. Ello obedece al entramado normativo aplicable, a la dificultad para comprender el funcionamiento específico de las autoridades y organismos, así como a las posibles barreras idiomáticas. Con lo anterior, el afectado se ve en la necesidad de solicitar el auxilio de un abogado, con el consiguiente coste económico. En definitiva, estas circunstancias pueden producir un efecto disuasorio, desincentivando el ejercicio de sus derechos o provocando el abandono de las solicitudes ya iniciadas.

IV. EL USO DE LAS NTIC PARA LA GARANTÍA DE LA SEGURIDAD PÚBLICA

La tecnología avanza a un ritmo que supera la capacidad de la legislación nacional e internacional para adaptarse y actualizarse. En no pocas ocasiones esta tecnología proviene de empresas privadas que desarrollan herramientas que, posteriormente, se implementan en el ámbito público. Por tanto, la sinergia entre los sectores públicos y los privados son cruciales.

En los últimos años, han proliferado sistemas de Inteligencia Artificial (IA) capaces de analizar grandes volúmenes de información, incluidos datos biométricos especialmente sensibles, como imágenes faciales, cuya utilización presenta un creciente interés para la seguridad pública y la investigación penal.

De hecho, la UE ha impulsado diversas reformas normativas dirigidas a incorporar estas capacidades tecnológicas en los mecanismos de cooperación policial. Así, ha reformado el Reglamento de Eurodac mediante el Reglamento 2024/1358, en vigor desde junio de 2026, y ha aprobado el Reglamento Prüm II, ambos con el propósito de permitir el tratamiento de imágenes faciales para el cumplimiento de sus fines asignados.

Asimismo, como ya se ha comentado, la UE ha adoptado el Reglamento 2024/1689 de Inteligencia Artificial (RIA), que permite la utilización de sistemas de identificación biométrica con fines de localización e identificación de determinados tipos de víctimas y de sospechosos o condenados. Con el fin de conciliar la protección de datos con las exigencias de seguridad pública, el RIA articula un enfoque basado en el riesgo y clasifica los sistemas de IA utilizados por las autoridades de cumplimiento de la ley en base a él. Desde esta perspectiva, los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público estarán permitidos bajo circunstancias estrictamente tasadas; los sistemas de identificación biométrica remota en diferido se califican como sistemas de alto

riesgo⁵; y los sistemas de identificación biométrica no remota están excluidos del ámbito de aplicación de esta norma.

Con carácter general los sistemas de identificación biométrica remota en tiempo real están prohibidos (art. 5.1, h), salvo que cuenten con autorización del órgano competente y sean empleados para localizar e identificar a víctimas de secuestro, trata de seres humanos o explotación sexual, desaparecidos y sospechosos de haber cometido alguno de los delitos consagrados en el Anexo II y castigados con al menos cuatro años de prisión (apartados 2 a 7 del art. 5). Los sistemas en diferido podrán ser utilizados para la búsqueda selectiva de una persona que ha cometido un delito o que ha sido condenada por ello (art. 26).

Otros sistemas de IA serán calificados de “alto riesgo” y estarán permitidos en la medida en que cumplan con las obligaciones asignadas en el RIA. A este grupo pertenecen las herramientas de IA que: evalúan el riesgo de que una persona sea víctima de delitos, apoyan el cumplimiento de la ley (como polígrafos), evalúan la fiabilidad de las pruebas, analizan rasgos y características de la personalidad, elaboran perfiles durante investigaciones o se utilizan para la categorización biométrica basada en atributo sensibles.

También destacan las herramientas predictivas (*predictive policing*) que tienen un enorme potencial para la mejora de la seguridad pública y la prevención de la comisión de delitos. Estas herramientas son utilizadas por las Fuerzas y Cuerpos de Seguridad españolas desde hace varios años. Entre ellas destacan VioGén –que evalúa el riesgo de las víctimas de violencia de género de volver a sufrir una agresión –y Veripol– que analiza el lenguaje empleado en las denuncias para detectar posibles denuncias falsas–.

El tratamiento de los datos personales por los sistemas de IA en el ámbito penal debe adecuarse a la Directiva 2016/680, como texto de referencia en esta materia.

Otro factor para tener en cuenta es que la incorporación de nuevas técnicas y funcionalidades exige una adecuada capacitación de los agentes de policía para su correcta utilización, que se centrará en dos elementos principales, formación técnica y competencia lingüística.

En España, el Ministerio del Interior se compromete a garantizar una educación completa y adecuada, asignando a agentes especializados la posición de Delegado de Protección de Datos de la Policía Nacional o de la Guardia Civil.

5. Según el art. 3.41 RIA los sistemas remotos son aquellos que identifican a las personas físicas sin su participación activa y generalmente a distancia, a través de comparaciones con bases de datos de referencia. Por sistema en tiempo real se refiere a aquellos en que la recogida de datos biométricos, su comparación e identificación se produce sin una demora (art. 3.42). Por sistemas en diferido serán todos los que no se encuadren en la clasificación anterior (art. 3.43).

El Reglamento SIS establece que, para asegurar la eficacia en el intercambio de información, se debe invertir en la formación de los usuarios, tanto antes de ser autorizados a tratar datos como de manera periódica posteriormente (art. 14). Una previsión similar se puede encontrar en el Reglamento Eurodac (Considerando 19) y en el Reglamento VIS (art. 28).

El Reglamento Prüm II subraya la importancia de la capacitación, especialmente, en materia de protección de datos (art. 63). Europol se compromete a brindar apoyo en la formación policial de los EEMM, en coordinación con CEPOL. El RIA también aborda la necesidad de que las personas reciban una formación adecuada en relación con su nivel de responsabilidad (art. 56).

Interpol promueve una formación digital en diferentes materias, incluida la protección de datos, ofreciendo una variedad de cursos a través de su Academia Virtual y organizando formaciones presenciales.

Esta formación no solo tiene que ser especializada, sino también continuada y actualizada, adaptándose a las novedades en la normativa de los instrumentos y avances en las herramientas tecnológicas. Además, la formación impartida a los miembros de la policía debe enfatizar especialmente los riesgos que pueden ocasionar sobre los datos personales de los sujetos involucrados en una investigación, especialmente en caso de que se produzca una brecha de seguridad.

Las NTIC se han constituido como herramientas esenciales para garantizar y reforzar la seguridad pública. La protección de la seguridad, en todas sus dimensiones, es un bien jurídico cuya salvaguarda persiguen todos los Estados. No obstante, este objetivo no puede justificar una utilización indiscriminada de cualquier tecnología. Al contrario, la creciente implantación de las NTIC ha ido acompañada de una mayor concienciación sobre los riesgos que estas pueden generar para los derechos fundamentales, lo que exige una actuación preventiva y proactiva tanto por parte de los Estados como de las instituciones supranacionales.

Por ejemplo, España debe adaptar el RIA a su ordenamiento jurídico previamente a su completa entrada en aplicación, lo que ocurrirá el 2 de agosto de 2026. Este proceso continúa actualmente en fase de tramitación a través del 121/000096 Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial, lo que evidencia los distintos ritmos existentes entre la innovación tecnológica y su regulación jurídica, pues existen sistemas de IA actualmente en funcionamiento.

V. CONSIDERACIONES FINALES Y RECOMENDACIONES

Tras exponer las principales conclusiones de este trabajo y evaluar las fortalezas y debilidades del sistema de protección de datos existente en el contexto de la

cooperación policial transfronteriza, se presentan las siguientes consideraciones y recomendaciones para abordar los desafíos pendientes.

1. Transformar la Directiva 2016/680 en un Reglamento de aplicación directa en todos los Estados miembros para la creación de un sistema único de protección de datos para todas las iniciativas, bases de datos, cuerpos o agencias que participan en la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
2. Los instrumentos de protección de datos deben actualizarse para incluir las especialidades derivadas de la aparición de instrumentos como el RIA y de aplicaciones como la identificación biométrica remota “en tiempo real”, las herramientas de *predictive policing* para evaluar riesgos de victimización o la reincidencia de los condenados.
3. Esta unificación del sistema de protección de datos simplificará el ejercicio de los derechos de acceso, rectificación, supresión y limitación del tratamiento, gracias al establecimiento de reglas únicas para su solicitud y concesión. Asimismo, esta medida debería complementarse con la creación de un punto de contacto único en cada Estado miembro que canalice todas las solicitudes relativas al tratamiento de datos personales en el marco de la cooperación policial transfronteriza. Esta misma solución sería aplicable a la remisión de solicitudes a Interpol cuando los datos del interesado sean objeto de tratamiento por este organismo internacional.
4. Resulta imprescindible garantizar un control efectivo de la rectificación y supresión de los datos personales, así como mantener una actualización permanente de la información objeto de transmisión. Con este fin, sería conveniente implantar sistemas de alertas automáticas que notifiquen a los Estados que hayan solicitado datos relativos a una determinada persona cualquier modificación, rectificación o supresión de estos. De este modo, las autoridades competentes podrán proceder a su actualización o, en su caso, a su eliminación en los procedimientos en los que dichos datos estén siendo tratados, asegurando así la exactitud, integridad y licitud del tratamiento de la información.
5. Adoptar estándares comunes globales, preferentemente mediante tratados internacionales o, en su defecto, acuerdos entre la UE y terceros países para asegurar una protección homogénea de los datos personales transmitidos. Cuando los datos se envían a países con protección insuficiente o inexistente, se pierde el control sobre su uso, lo que abre la puerta a su posible explotación para finalidades distintas de la seguridad pública, como mercadotecnia, sanidad o seguros.

Para evitarlo, también se recomienda aplicar técnicas informáticas que restrinjan el tratamiento de los datos y garanticen su trazabilidad. Además, los Estados miembros, los instrumentos de cooperación y el Supervisor Europeo de

Protección de Datos (SEPD) deben reforzar el control periódico sobre la conservación de los datos compartidos.

6. Con el objetivo de minimizar los riesgos, resulta aconsejable incorporar técnicas informáticas que limiten el tratamiento de los datos a los fines autorizados y permitan su trazabilidad durante todo su ciclo de vida. Asimismo, los Estados miembros, los instrumentos de cooperación y el Supervisor Europeo de Protección de Datos (SEPD) deben reforzar los mecanismos de supervisión y control periódico sobre la conservación, actualización y supresión de los datos compartidos, verificando el cumplimiento efectivo de los principios y garantías establecidos en la normativa aplicable.

BIBLIOGRAFÍA BÁSICA

BLASI CASAGRÁN, C.: «Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU», *Human Rights Law Review*, n.º 21, 2021, pp. 433-457.

BOEHM, F.: *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer, 2012.

BURGORGUE-LARSEN, L.: «Las víctimas del delito en el proceso penal internacional: ejemplo de la Corte Penal Internacional», *Revista Jurídica*, n.º 12, 2005, pp. 9-32.

COTINO HUESO, L.: «Riesgos e impactos del big data, la inteligencia artificial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho», *Revista General de Derecho Administrativo*, n.º 50, 2019.

CUSTERS, B.: «Technology in policing: Experiences, obstacles and police needs», *Computer law & security review*, n.º 28, pp. 62-68.

DE HERT, P. y PAPAKONSTANTINO, V.: «The new police and criminal justice data protection directive: a first analysis», *New Journal of European Criminal Law*, Vol. 7, 2016, pp. 7-19.

DIMITROVA, D. y DE HERT, P.: «The Right of Access Under the Police Directive: Small Steps Forward», *Privacy Technologies and Policy: 6th Annual Privacy Forum*, Heidelberg, Springer, 2018, pp. 111-130.

DIMITROVA, D.: «Article 16 Right to Rectification or Erasure of Personal Data and Restriction of Processing», en KOSTA, E. y BOEHM, F. (dir.): *The EU Law Enforcement Directive (LED): A Commentary*, 2024, pp. 293-308.

DONAIRE VILLA, F.J.: «Solidaridad normativa y derechos fundamentales en el Código de Fronteras Schengen», *Revista Vasca de Administración Pública*, n.º 128-II, 2024, pp. 127-262.

DRECHSLER, L.: «Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context», *International Data Privacy Law*, vol. 11, n.º 2, 2021, pp. 182-195.

FERNÁNDEZ DEL CASADEVANTE ROMANÍ, C.: *International Law of Victims*, Heidelberg, Springer, 2012.

GONZÁLEZ FUSTER, G.: *The emerge of personal Data Protection as a Fundamental Right of the EU*, Springer, 2014.

GRZELAK, A.: «Protection of Personal Data of Crime Victims in European Union Law– Latest Developments», XXXVIII *Polish Yearbook of International Law*, 2018, pp. 209-228.

GUTIÉRREZ ZARZA, Á.: *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Springer, 2015.

JIMENA QUESADA, L. y TOMÁS MALLÉN, B.: *Justicia y anonimización de datos personales*, Tirant lo Blanc, 2021.

JIMENA QUESADA, L.: «Configuración constitucional de las FFCCS españoles en el marco de la Unión Europea», *Revista Vasca de Administración Pública*, n.º 49, 1997, pp. 167-213.

JOH, E.: «The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing», *UC Davis Legal Studies Research*, 2015 pp. 15-42.

LEISER M. y CUSTERS, B.: «The law enforcement Directive: Conceptual challenges of UE Directive 2016/680», *European Data Protection Law Review (EDPL)*, vol. 5, n.º3, p. 368-375.

MARTÍNEZ ALARCÓN, M. L.: «El principio de subsidiariedad en el Tratado de Lisboa», *Parlamento y Constitución. Anuario*, n.º 13, 2010, pp. 164-198.

PLANCHADELL GARGALLO, A.: «Publicidad del proceso e intimidad de la víctima: una aproximación desde el Estatuto de la Víctima del Delito», *Teoría&Derecho*, 2018, n.º 24, pp. 151-177.

QUINTEL, T. y MITSILEGAS, V.: «Article 6 Distinction between Different Categories of Data Subject», en KOSTA, E. y BOEHM, F. (dir.): *The EU Law Enforcement Directive (LED): A Commentary*, 2024, pp. 165-180.

QUINTEL, T.: *Connecting Personal Data of Third Country Nationals: Interoperability of EU databases in the light of the CJEU's case law on data retention*, 2018.

RIDAURA MARTÍNEZ, M. J.: «La seguridad ciudadana como función del Estado», *Estudios de Deusto*, vol. 62, n.º 2, 2014, pp. 319-346.

SERRA CRISTÓBAL, R.: «Los derechos de la víctima en el proceso vs. Medios de comunicación. Un ejemplo en la información sobre delitos de violencia contra la mujer», *Revista Española de Derecho Constitucional*, n.º 103, 2015, pp. 199-212.

TOMÁS MALLÉN, B., GARCÍA MAHAMUT, R., y PAUNER CHULVI, C. (Eds.): *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español. Cuestiones clave de orden nacional y europeo*, Valencia, Tirant lo Blanch, 2021.

TOMÁS MALLÉN, B.: «Derechos fundamentales y *Drittwirkung* en perspectiva multinivel: desarrollos recientes en el Derecho europeo», *Revista de Derecho Político*, n.º 115, 2022, pp. 207-235.

VAVOULA, N.: «Interoperability of EU Information System: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals», *European Public Law*, 2020, pp. 131-156.

VIGURI CORDERO, J. A.: *Seguridad y Protección de Datos en el Sistema Europeo Común de Asilo*, Tirant lo Blanch, 2020.
