La digitalización de la cooperación judicial en la UE a través de eu-LISA: avances, virtualidades e incertidumbres del nuevo sistema de justicia penal en Red [1*]

Valentina Faggiani

Departamento de Derecho Constitucional
Universidad de Granada
valenf@ugr.es

Abstract
The digitalisation of judicial cooperation in criminal matters and police cooperation is one of the priorities of the EU strategy on e-Justice 2024-2028. The heart of this system is eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (AFSJ), and the collaborative relationship with other bodies in this field, in particular Eurojust and Europol. In this framework, the study, after examining the role of eu-LISA, will focus on the main legislative instruments adopted in the Union between 2022 and 2025 to promote this process, which place this Agency and the collaboration with Eurojust and Europol at the centre.

Keywords: digitalisation, judicial cooperation in criminal matters and police cooperation, Eu-LISA, Eurojust, Europol

[1] * Este trabajo se enmarca en los siguientes proyectos: Módulo Jean Monnet, "*Challenges to Justice in the EU: Perspectives for Reform*", 2022-2025, ref. 101085462; Módulo Jean Monnet, "Desafíos y perfiles estratégicos de la UE en la lucha contra el crimen organizado" (RUECO) 2023-2026, ref. 101127315; y Proyecto de investigación I+D+i "Proceso Penal y Espacio de Libertad, Seguridad y Justicia: Garantías, Cooperación Transfronteriza y Digitalización", PID2023-152074NB-I00.

Eu-LISA como centro neurálgico de los sistemas informáticos de gran magnitud y la coordinación con Eurojust y Europol

La digitalización de la cooperación judicial en materia penal y de la cooperación policial se ha convertido en una de las prioridades de la estrategia de la UE sobre la justicia en Red[2], pues sus potencialidades pueden transformar la forma de gestionar las relaciones entre los operadores jurídicos de los Estados miembros y también con los países terceros[3].

El corazón de este sistema se encuentra en eu-LISA[4], la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (ELSJ), y en la relación de colaboración, que ha conseguido establecer con los demás organismos en este ámbito. Por ello, el presente trabajo, tras analizar el rol de esta Agencia, se centrará en los principales instrumentos legislativos aprobados en el seno de la Unión entre 2022-2025 para promover este proceso.

El estudio de eu-LISA y de su relación con las demás Agencias de la UE responde a la necesidad de conocer con más detalle estas entidades, que son parte integrante de su cuerpo administrativo[5], a fin de comprender las funciones y los perfiles contradictorios, así como las permanentes tensiones entre la perspectiva supranacional y los elementos intergubernamentales, que siguen persistiendo. Estos aspectos limitan la construcción de una real "integración descentralizada"[6], es decir, el desarrollo y la concreta actuación de sistemas de cooperación basados en la creación de "redes"[7], como en el caso de las agencias, cuyo objetivo es implementar las políticas comunitarias[8]. Este enfoque permite además reflexionar sobre si el uso y la aplicación

[2] *Vid.* Consejo 2025. En línea con la anterior estrategia correspondiente al periodo 2019-2023, tres son los objetivos esenciales en dicho marco: a. el acceso a la información en el ámbito de la justicia; b. las comunicaciones electrónicas entre las autoridades judiciales, la ciudadanía y los profesionales de la Justicia, y c) la interoperabilidad entre aplicaciones y ámbitos judiciales. Ya la Comisión Europea en 2020 hacía hincapié en que el acceso a la tutela judicial y a la cooperación entre los Estados miembros se encuentran entre los principales objetivos de la UE en el ELSJ.

[3] Con respecto a la digitalización del proceso penal en la UE, *vid.* Arangüena Fanego, De Hoyos Sancho, Pillado González (dirs.) 2023.

[4] Reglamento (UE) 2018/1726 de 14 de noviembre de 2018 relativo a la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), y por el que se modifican el Reglamento (CE) n. 1987/2006 y la Decisión 2007/533/JAI del Consejo y se deroga el Reglamento (UE) n. 1077/2011, PE/29/2018/REV/1, DO L 295 de 21.11.2018.

[5] Sobre las agencias de la UE, v. Chiti 2013, 93-110; Alberti 2018; Pi Llorens 2017, 77-117.

[6] Chiti 2015, 909-984.

[7] Barbieri 2007, 80. El autor describe a las agencias también como "*punti focali (nodi) di una rete di relazioni interistituzionali"* que ponen en marcha *"modalità di coordinamento (formali ed informali)*" (94).

[8] Akbik, Freudlsperger, Migliorati 2024, 645-670.

de la tecnología respetan los derechos fundamentales de las personas involucradas en un proceso penal, siendo muy marcada la confrontación entre seguridad *vs.* protección de datos personales.

Eu-LISA es una agencia reguladora, un organismo dotado de personalidad jurídica, y por lo tanto de "autonomía jurídica, administrativa y financiera"[9], con sede en Tallin, en Estonia, si bien las funciones relacionadas con el desarrollo y la gestión operativa se llevan a cabo en Estrasburgo, en Francia. En dicha Agencia se concreta la "delegación de las competencias operativas" de la UE, y más concretamente de la Comisión Europea, es decir de la competencia de ejecución en los ámbitos, en que los Estados miembros han decidido compartir competencias con la Unión[10]. Este proceso de descentralización, que ha llevado a una proliferación de las agencias, ha impulsado la "transformación institucional", incidiendo en la estructura del sistema[11].

Y más en este caso concreto, en el que el intercambio estructurado de datos en el ámbito de los distintos sistemas de información de gran magnitud a través del diálogo entre centro y periferia está creando un nuevo modelo de gestión de las relaciones en sectores tan sensibles como la inmigración y el asilo, la cooperación judicial en materia civil y penal y la cooperación policial. Por otra parte, y aquí reside el perfil más inquietante, si bien estos organismos hayan adquirido importantes poderes, que se ejercen de forma casi autárquica, no existen mecanismos de control verdaderamente incisivos, que puedan contrarrestar de forma eficaz e inmediata eventuales extralimitaciones.

Eu-LISA, instituida en 2011, a fin de reforzar la cooperación entre los Estados miembros, actualmente se encarga de la gestión operativa de los sistemas informáticos de gran magnitud en el ELSJ[12], es decir de llevar a cabo "todas las funciones necesarias para el mantenimiento" de su funcionamiento, con la inclusión de la responsabilidad de las infraestructuras de comunicación, que utilicen.

Tales sistemas informáticos son:

- SIS II, el Sistema de Información de Schengen de segunda generación
- VIS, Sistema de Información de Visados
- EURODAC, el Sistema Europeo de Comparación de Impresiones Dactilares de los solicitantes de asilo

[9] Considerando n. 5 del Reglamento de eu-LISA.

[10] En este sentido, v. Tassinari 2023.

[11] Barbieri, *op. cit.*, 77.

[12] Sus bases normativas se encuentran en los artículos 74, 77, ap. 2, a) y b), 78, ap. 2, e), 79, ap. 2, c), 82, ap. 1, d), 85, ap. 1, 87, ap. 2, a), y 88, ap. 2, del TFUE. La extensión del mandato de eu-LISA ha sido facilitada por la inexistencia de una definición de sistemas de gran magnitud.

- EES, el Sistema de Entradas/Salidas[13]
- DubliNet, el Sistema para la transmisión de las solicitudes de asilo en la UE
- ETIAS, el Sistema Europeo de Autorización de Viajes
- API, el Sistema para la recogida y la transmisión de información anticipada sobre los pasajeros[14]
- ECRIS-TCN y la aplicación de referencia ECRIS, el Sistema Europeo de Información de Antecedentes Penales — Nacionales de Terceros Países[15]
- e-CODEX, el sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal
- la plataforma de colaboración de los equipos conjuntos de investigación (ECI)
- y el enrutador Prüm II.

El objetivo de eu-LISA es garantizar la interoperabilidad[16], es decir asegurar un mejor acceso a la información almacenada en distintos sistemas de información de la UE y la gestión de la identidad a escala de la Unión. Su mandato operativo puede ser además ampliado ulteriormente, si se establece en los actos jurídicos de la UE, atendiendo a los artículos 67 a 89 TFUE. No obstante, es importante poner de relieve que estos sistemas "no intercambiarán datos ni permitirán compartir información o conocimientos, salvo que se disponga de manera específica en un acto jurídico de la Unión"[17]. Esto significa que eu-LISA no "fusiona" los distintos sistemas ni realiza un uso compartido de la información[18]. Es decir, los Estados siguen gestionando sus datos a nivel central, aunque después estos sistemas, precisamente a través de esta Agencia, acaban conectándose, por su carácter descentralizado.

[13] El sistema EES empezó a funcionar el 12 de octubre de 2025, si bien su implementación, a través de la recogida de datos personales, es decir, escaneo de las impresiones dactilares y fotografía de la cara será gradual hasta el 20 de abril de 2026, cuando su aplicación será plena. Se trata, en definitiva, de un paso muy importante en la digitalización de las fronteras exteriores, que sustituirá el pasaporte en papel por un sistema de registración electrónico. De esta forma, se pretende facilitar la identificación de las personas y contribuir a prevenir supuestos de delincuencia grave. Al respecto, v. Decisión de Ejecución (UE) 2025/1544 de la Comisión de 30 de julio de 2025 por la que se determina la fecha en que entrará en funcionamiento el Sistema de Entradas y Salidas de conformidad con el Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, DOUE, n. 1544, 31.7.2025.

[14] Reglamento (UE) 2025/12 del Parlamento Europeo y del Consejo de 19 de diciembre de 2024 relativo a la recogida y la transferencia de información anticipada sobre los pasajeros para reforzar y facilitar las inspecciones en las fronteras exteriores, por el que se modifican los Reglamentos (UE) 2018/1726 y (UE) 2019/817 y se deroga la Directiva 2004/82/CE del Consejo, E/68/2024/REV/1, DO L, 2025/12, 8.1.2025.

[15] Di Paolo 2019, 3380-3384.

[16] Tassinari 2022, 291-338.

[17] Art. 1, par. 6, del Reglamento de eu-LISA.

[18] Illamola Dausà 2015, 109.

Para controlar la calidad de los datos introducidos en los sistemas, que gestiona, y sin perjuicio de la responsabilidad de los Estados, a eu-LISA le corresponde establecer mecanismos y procedimientos automatizados, indicadores comunes y normas de calidad mínimas relativas al almacenamiento de la información. A tal efecto, se establece un repositorio central, que contenga únicamente datos anonimizados para informes y estadísticas[19]. Además, cuando se haya previsto la interoperabilidad de los sistemas informativos de gran magnitud, desarrolla las acciones necesarias[20] y realiza el seguimiento de la investigación para la gestión operativa de estos sistemas, y puede llevar a cabo proyectos piloto[21].

Y, por último, eu-LISA presta apoyo a los Estados miembros y a la Comisión para asesorarlos sobre la "conexión de sus sistemas nacionales a los sistemas centrales de los sistemas informáticos de gran magnitud" del ELSJ[22]. Asimismo, los Estados miembros pueden presentar una solicitud de asistencia *ad hoc* de forma individual a la Comisión por necesidades extraordinarias de seguridad o de migración. Por su parte, la Comisión podrá pedir a la Agencia que le "preste asesoramiento o apoyo" "sobre cuestiones técnicas relacionadas con sistemas existentes o nuevos, en particular mediante estudios y pruebas"[23].

Si bien eu-LISA se puede considerar como el centro neurálgico de la gestión operativa de los sistemas informáticos de gran magnitud en el ELSJ, su concreto funcionamiento depende también de la cooperación con las distintas Agencias en este ámbito, como Eurojust, la Agencia de la UE especializada en la cooperación judicial en materia penal[24], y Europol, la Agencia de la UE para la cooperación en materia policial[25]. Las sinergias, que se han desarrollado entre tales organismos, han permitido realizar un importante trabajo para acelerar la transformación digital y la adopción de soluciones informáticas basadas en la IA en el ámbito de la Justicia y los Asuntos de Interior (JAI), sentando las bases para la aplicación de sistemas digitales a tales ámbitos.

[19] Art. 12 del Reglamento de eu-LISA.
[20] Art. 13 del Reglamento de eu-LISA.
[21] Art. 14 del Reglamento de eu-LISA.
[22] Considerando n. 8 del Reglamento de eu-LISA.
[23] Art. 16 del Reglamento eu-LISA.
[24] Reglamento (UE) 2018/1727 de 14 de noviembre de 2018 sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo, OJ L 295, 21.11.2018. Al respecto, *vid.*: Faggiani 2021, 185-210.
[25] Reglamento (UE) 2016/794 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.

Esta cooperación, prevista de forma expresa en el Reglamento de eu-LISA, en el que se ha establecido la participación en calidad de observadores en las reuniones de su Consejo de Administración, que tienen lugar dos veces al año, ha sido potenciada gracias a la firma de interesantes *Memoranda of Understanding (MoU)*, fruto de un diálogo constante[26]. Tanto Europol como Eurojust han estipulado acuerdos de este tipo respectivamente en 2016 y 2017[27] con el objetivo de actualizar conjuntamente los sistemas y procesos digitales existentes y establecer otros nuevos, modernizando el funcionamiento de la justicia penal y mejorando la cooperación judicial en la UE.

En ambos casos las Agencias involucradas se han comprometido a cooperar mediante el intercambio de conocimientos especializados y mejores prácticas en la aplicación de sus respectivos mandatos y, cuando sea pertinente, en actividades y servicios relacionados con las TIC, y en asuntos estratégicos y administrativos, como programas de trabajo, estrategias y planes de acción. En el memorándum entre eu-LISA y Europol se hace referencia expresa también al deber de cooperar en la investigación y el seguimiento de la evolución de las iniciativas de este tipo, entre otras cosas en materia de seguridad informática y cibernética, certificación, normalización, uso de la biometría, continuidad de las actividades y análisis de incidentes[28] y a la importancia de la formación impartida a los Estados miembros y al personal de Europol y eu-LISA.

Esta proficua colaboración, que se ha desarrollado antes en el plano operativo, desde la implementación de actos de *soft law*, buenas prácticas y protocolos, se ha concretado en la adopción de interesantes medidas legislativas, que constituyen parte integrante del paquete de digitalización de la justicia[29], y en la regulación en el Reglamento sobre la IA de los sistemas de reconocimiento biométrico en actividades de *law enforcement*[30].

---

[26] Art. 22 del Reglamento eu-LISA.

[27] MoU between Europol and eu-LISA, 22.3.2016, https://www.eulisa.europa.eu/PartnersStakeholders/Documents/MoU_Europol_eu-LISA.pdf; MoU between Eurojust and eu-LISA, 19.9.2017, https://www.eurojust.europa.eu/document/memorandum-understanding-between-eurojust-and-eu-lisa. El MoU entre eu-LISA y Eurojust fue implementado a través del plan de cooperación 2021-2023, de 11 de octubre de 2021, que ha puesto en marcha actividades conjuntas sobre sectores de interés mutuo https://www.eurojust.europa.eu/document/cooperation-plan-2021-2023-eurojust-and-eu-lisa. La necesidad de fortalecer ulteriormente la cooperación en la digitalización se ha puesto de relieve también en Eurojust 2024. Sobre la cooperación entre eu-LISA y Eurojust, v. Faggiani 2024.

[28] Art. 4 del MoU eu-LISA-Europol.

[29] Comisión Europea 2.12.2020.

[30] Art. 5 del Reglamento (UE) 2024/1689 de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial), PE/24/2024/REV/1, DO L, 2024/1689, 12.7.2024.

2. La plataforma sobre los equipos conjuntos de investigación como instrumento estratégico en la lucha contra la delincuencia organizada

La cooperación entre eu-LISA y Eurojust se ha formalizado en el Reglamento relativo a la institución de una plataforma de colaboración para los Equipos Conjuntos de Investigación (ECI) y el Reglamento relativo al Sistema de Gestión de Casos de Eurojust rediseñado, dotado de componentes basados en IA.

Los ECI[31] se constituyen en virtud de un acuerdo entre las autoridades competentes de dos (actuación bilateral) o más Estados (actuación multilateral), con el fin de llevar a cabo investigaciones penales. Suelen trabajar por un período, que oscila entre 12 y 24 meses, dependiendo de la complejidad del asunto de que se trata y por lo tanto del tiempo, que requiere la investigación. Estos mecanismos, que permiten a las autoridades judiciales, policiales y aduaneras de dos o más Estados miembros, y en algunos casos de terceros países, cooperar y comunicar de forma directa, responden a una estrategia común de investigación, siendo uno de los instrumentos más avanzados de cooperación judicial en materia penal. Se asiste a un foro de trabajo para jueces y fiscales y autoridades de policía.

La institución de una plataforma, como la prevista por el Reglamento (UE) 2023/969[32], puede facilitar enormemente la colaboración entre los integrantes de los ECI en la organización de la "investigación e instrucción en el proceso penal"[33] de delitos transfronterizos, como la ciberdelincuencia, el terrorismo y la delincuencia grave y organizada, reduciendo procedimientos y trámites largos.

La necesidad de una medida de este tipo fue impulsada por el rol de relieve adquirido por Eurojust en la cooperación judicial en materia penal y luego acelerada tras la adopción del Reglamento (UE) 2022/838[34], que atribuyó a

[31] V. Decisión marco del Consejo de 13 de junio de 2002 sobre equipos conjuntos de investigación, OJ L 162, 20.6.2002. Atendiendo al art. 1 de la presente Decisión marco: "Las autoridades competentes de dos o más Estados miembros podrán crear de común acuerdo un equipo conjunto de investigación, con un fin determinado y por un período limitado que podrá ampliarse con el consentimiento de todas las partes, para llevar a cabo investigaciones penales en uno o más de los Estados miembros que hayan creado el equipo".

[32] Reglamento (UE) 2023/969 de 10 de mayo de 2023 por el que se establece una plataforma de colaboración en apoyo del funcionamiento de los equipos conjuntos de investigación y se modifica el Reglamento (UE) 2018/1726, PE/73/2022/REV/1, OJ L 132, 17.5.2023. El presente Reglamento se ha adoptado en virtud del art. 82, ap. 1, pár. seg., d., del TFUE.

[33] Considerando n. 3 del Reglamento (UE) 2023/969.

[34] Reglamento (UE) 2022/838 de 30 de mayo de 2022 por el que se modifica el Reglamento (UE) 2018/1727 en lo que respecta a la preservación, análisis y almacenamiento en Eurojust de pruebas relativas al genocidio, los crímenes contra la humanidad, los crímenes de guerra

esta Agencia la función de preservar, analizar y conservar en una instalación de gestión y almacenamiento automatizado de datos temporales, las pruebas relativas al genocidio, los crímenes contra la humanidad, los crímenes de guerra y las infracciones penales conexas. De esta forma, se ha permitido el intercambio de pruebas relacionadas con las autoridades nacionales competentes y las autoridades judiciales internacionales, en particular la Corte Penal Internacional, a fin de garantizar que los autores de los crímenes cometidos en Ucrania no se queden impunes, sino que rindan cuentas[35]. A raíz de esta modificación, en julio de 2023, se instituyó un Centro para la persecución del crimen de agresión contra Ucrania gestionado por Eurojust, que funciona, a través de los equipos de investigación, que pueden colaborar de forma voluntaria.

El objetivo de la plataforma de colaboración para los ECI es facilitar el intercambio de información y realizar la comunicación, indicando el *modus procedendi*. Se trata de un sistema instrumental para permitir a la UE elaborar una "respuesta coordinada" a las actividades delictivas y prestar apoyo a los Estados miembros en la lucha contra la criminalidad. La plataforma informática de colaboración de los ECI, que tendrá carácter voluntario, estará alojada en eu-LISA, que será responsable del diseño de la arquitectura física, del desarrollo conforme al principio de protección de datos desde el diseño y por defecto[36], de la gestión operativa para asegurar su mantenimiento y del correcto funcionamiento[37], utilizando las funciones existentes de SIENA (Red de Intercambio Seguro de Información) y otras funciones de Europol para garantizar la complementariedad y, si ha lugar, la conectividad[38].

La plataforma se compondrá de:

> a) un sistema de información centralizado, que permita el almacenamiento temporal de datos por el tiempo necesario para transferirlos. Dicha información tendrá que ser suprimida de forma automática y permanente, una vez descargada por todos los destinatarios;
> b) un soporte lógico (*software*) de comunicación, que permita el almacenamiento local seguro de datos en los dispositivos de los usuarios;

y las infracciones penales conexas, OJ, n. 148, 31.5.2022. En concreto, se modificó el art. 4, ap. 1, del Reglamento (UE) 2018/1727. Al margen de su importancia en el marco del conflicto en Ucrania, esta reforma ha dotado a Eurojust de mayor relevancia en la lucha contra los supuestos de criminalidad grave transfronteriza. Torres Pérez 2022, 1-17.

[35] Eurojust cuenta desde 2016 con un acuerdo de colaboración con Ucrania, en virtud del cual un fiscal de enlace de este país se encuentra en Europa para facilitar la cooperación.

[36] Signorin 2025, 206-221.

[37] Art. 7 del Reglamento (UE) 2023/969.

[38] Considerando n. 22 del Reglamento (UE) 2023/969.

> c) una conexión entre el sistema de información centralizado y las herramientas informáticas pertinentes, que apoyen el funcionamiento de los ECI, y sean gestionadas por la Secretaría de la red de ECI.

A través de esta herramienta se pretende alcanzar los siguientes objetivos[39]:

> a. facilitar la coordinación y la gestión de los ECI
> b. favorecer el intercambio rápido y seguro y el almacenamiento temporal de datos operativos, con la inclusión de archivos voluminosos, mediante una función de carga y descarga, y de datos no operativos entre los usuarios
> c. asegurar comunicaciones seguras mediante una función que comprenda mensajería instantánea, chat, audioconferencia y videoconferencia
> d. permitir la trazabilidad de los intercambios de pruebas, usando un mecanismo avanzado de registro y de seguimiento, así como del acceso a ellas y de su tratamiento
> e. evaluar a los ECI, a través de un proceso colaborativo específico.

La Comisión Europea, en junio de 2025, adoptó la Decisión de Ejecución (UE) 2025/1274[40] para facilitar la activación de la plataforma de colaboración. Eu-LISA pondrá el soporte lógico (*software*) de comunicación a disposición de los usuarios de dicha plataforma, impartirá formación sobre su uso técnico a la secretaría de la red de ECI, suministrando también material de formación, y creará un servicio de atención para responder a las consecuencias de eventuales incidentes técnicos.

En dicho marco, los ECI se conciben como un espacio en el que los usuarios pueden entrar previa autorización del administrador/es, que gestiona/n el acceso a las fases operativas y posoperativa, de conformidad con el acuerdo que se estipulará[41]. Cada ECI solo podrá contar con un espacio de colaboración, que eu-LISA creará al efecto, tras haber recibido el correspondiente acuerdo sobre ECI. Dichos espacios no interactuarán[42].

En dicho marco, por lo tanto, será fundamental asegurar la seguridad del intercambio de datos a través del uso de "sólidos algoritmos de cifrado extremo para cifrar los datos en tránsito o reposo"[43]. Los datos operativos de

[39] Art. 5 del Reglamento (UE) 2023/969.

[40] Decisión de Ejecución (UE) 2025/1274 de la Comisión de 30 de junio de 2025 por la que se establecen disposiciones de aplicación del Reglamento (UE) 2023/969 del Parlamento Europeo y del Consejo en lo que respecta a las medidas necesarias para la ejecución técnica de la plataforma de colaboración de los equipos conjuntos de investigación, C/2025/3827, DO L, 2025/1274.

[41] Considerando n. 29 del Reglamento (UE) 2023/969.

[42] Art. 1 de la Decisión de Ejecución (UE) 2025/1274.

[43] Considerando n. 30 del Reglamento (UE) 2023/969.

los ECI se conservarán en el sistema de información centralizado el tiempo necesario para su descarga por parte de los usuarios de dicha plataforma. Tras este proceso, o una vez expirado el período de conservación, los datos serán suprimidos automáticamente y de forma permanente del sistema de información centralizado[44]. Los datos no operativos se almacenarán hasta la conclusión de la evaluación del ECI y, de todas formas, durante no más de cinco años desde su ingreso en la plataforma. Si no se previera la evaluación o tras la expiración del período de conservación se eliminarán automáticamente del sistema informático centralizado[45].

Son responsables del tratamiento de datos personales: la autoridad nacional competente de un Estado miembro y, según proceda, Eurojust, Europol, la Fiscalía Europea, la OLAF o cualquier otro órgano u organismo de la Unión. Además, se designará un administrador del espacio de los ECI como responsable cuando en la plataforma de colaboración de los ECI participen terceros países o representantes de autoridades judiciales internacionales[46].

Eu-LISA se encargará del tratamiento de datos personales, que se intercambien a través de la plataforma de colaboración de los ECI y se almacenen en ella. A tal fin, tendrá que asegurar el registro del acceso al sistema y de todas las operaciones de tratamiento de datos para controlar la integridad y la seguridad de los datos y la legalidad de tales procesos y llevar a cabo la supervisión interna. La Agencia no tendrá acceso a los datos operativos y no operativos almacenados en los espacios de colaboración de los ECI[47] y tendrá que respetar el secreto profesional y las obligaciones de confidencialidad. Los usuarios de la plataforma serán considerados corresponsables del tratamiento de los datos personales no operativos. El control y la evaluación del cumplimiento de las obligaciones de eu-LISA se realizará atendiendo a los distintos informes[48], los cuales constituyen el principal instrumento en este sentido.

Asimismo, se prevé la responsabilidad de los Estados miembros, Eurojust, Europol[49], la Fiscalía Europea, la OLAF o cualquier otro órgano u organismo competente de la Unión por los daños ocasionados a la plataforma de colabo-

[44] Art. 21 del Reglamento (UE) 2023/969.
[45] Art. 22 del Reglamento (UE) 2023/969.
[46] Art. 23 del Reglamento (UE) 2023/969.
[47] Considerando n. 37 del Reglamento (UE) 2023/969.
[48] Sobre los informes, que tienen que presentar eu-LISA y la Comisión para el seguimiento del desarrollo y el funcionamiento de la plataforma de ECI, se reenvía al considerando n. 23 y n. 38 y al art. 26 del Reglamento (UE) 2023/969.
[49] En relación con Europol, v. por ejemplo la STJUE (GS), de 5 de marzo de 2024, C-755/21 P, *M. Kočner c. Europol*, en la que se anula la STG de 29 de septiembre de 2021, *Kočner/Europol*, T-528/20, y se condena a Europol a indemnizar a la recurrente por los daños sufridos por la divulgación de datos personales y la inclusión de su nombre en las "listas de mafiosos".

ración de los ECI por el incumplimiento de sus obligaciones, salvo que eu-LISA no haya adoptado medidas razonables para evitar que se produzcan esos daños o para minimizar sus consecuencias. En el caso de que la responsabilidad sea del Estado se aplicará el Derecho nacional de dicho Estado miembro y en los demás supuestos los actos constitutivos de los demás organismos[50].

En cuanto a su gestión interna, el Consejo de Administración, es decir, el órgano ejecutivo de eu-LISA, constituirá el Consejo de Administración del Programa, que se encargará de la gestión de la fase de diseño y del desarrollo de la plataforma[51]. El Consejo de Administración del Programa presentará al Consejo de Administración de eu-LISA informes por escrito de forma periódica y, cuando sea posible, cada mes, sobre los avances. No tendrá competencias para adoptar decisiones ni mandato alguno de representación de los miembros del Consejo de Administración de la Agencia eu-LISA. Asimismo, eu-LISA creará el Grupo consultivo para adquirir conocimientos especializados y preparar el programa de trabajo y el informe anuales de actividad de la agencia[52]. Este Grupo se compondrá de representantes de los Estados miembros, la Comisión y la Secretaría de la red de ECI y estará presidido por eu-LISA. Y, por último, es interesante observar que, mientras Irlanda se ha adherido a esta medida, Dinamarca, como de costumbre, no ha participado en la adopción ni queda vinculada ni sujeta a su aplicación[53].

3. El sistema de gestión de casos de terrorismo

También el sistema de gestión de casos de terrorismo, instituido por el Reglamento (UE) 2023/2131, de 4 de octubre de 2023, que modifica el Reglamento de Eurojust[54], se basa en un sistema informático descentralizado para el intercambio seguro de datos, que estará conectado a una red de sistemas informáticos (*back-end*) y puntos de acceso e-CODEX interoperables[55].

[50] Art. 20 del Reglamento (UE) 2023/969.

[51] Considerando n. 28 del Reglamento (UE) 2023/969.

[52] Art. 12 del Reglamento (UE) 2023/969.

[53] Art. 3 del Protocolo n. 21 sobre la posición del Reino Unido y de Irlanda respecto del ELSJ, anejo al TUE y al TFUE; y artículos 1 y 2 del Protocolo n. 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE.

[54] V. en particular el art. 22 bis del Reglamento (UE) 2023/2131 de 4 de octubre de 2023 por el que se modifican el Reglamento (UE) 2018/1727 y la Decisión 2005/671/JAI del Consejo en lo que respecta al intercambio de información digital en casos de terrorismo, OJ L, 11.10.2023. Eurojust 2022.

[55] Reglamento (UE) 2022/850 de 30 de mayo de 2022 relativo a un sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal (sistema e-CODEX), y por el que se modifica el Reglamento (UE) 2018/1726, OJ L 150, 1.6.2022. El sistema e-CODEX, en línea con el principio de interoperabilidad, permite al sector de la justicia conectarse a los sistemas informáticos

El objetivo es facilitar la trasmisión de informaciones entre las autoridades de los Estados miembros y, en su caso, de los terceros países a Eurojust para que pueda descubrir determinados nexos entre procedimientos judiciales transfronterizos contra sospechosos de delitos de terrorismo, y trasladar la información tratada en Eurojust relativa a otros casos de delitos graves, que requieren de la adopción de medidas de cooperación[56].

En efecto, una persona sospechosa o investigada en un caso pendiente en un Estado miembro podría haber estado involucrada en un asunto ya finalizado en otro Estado miembro, tanto con sentencia de condena como con absolución o sobreseimiento, y también pueden existir nexos entre investigaciones o instrucciones que de otra manera no se habrían podido apreciar, siendo necesario conservar los datos relativos a todo tipo de investigación, no solo las que han finalizado con una condena.

Por ello, es muy importante tener en cuenta el carácter dinámico y globalizado de la criminalidad trasnacional, que puede afectar a dos o más Estados y puede ser descubierto en un segundo momento, imponiendo la institución de formas de coordinación y colaboración entre las autoridades competentes[57]. Para ello, estas "necesitan saber exactamente qué tipo de información deben transmitir, en qué fase del proceso penal nacional y en qué" supuestos[58]. Además, dicha información tiene que ser intercambiada de forma estructurada, organizada, sistemática y semiautomatizada, es decir en parte automatizada y en parte controlada por personas[59].

El nuevo sistema de gestión de casos "modernizado" tiene que integrar, mejorar y facilitar el Registro Judicial Antiterrorista Europeo (*Counter-Terrorism Register*, CTR)[60], supliendo sus deficiencias. En efecto, al haberse instituido después de la adopción del Reglamento de Eurojust, el Reglamento (UE) 2018/1727, dicha normativa no lo mencionaba ni está integrado en su

---

de las autoridades nacionales competentes, como el poder judicial, u otras organizaciones. Atendiendo al art. 3.1 del Reglamento (UE) 2022/850, se entiende por sistema e-CODEX (sistema de comunicación para la justicia digital mediante intercambio electrónico de datos) un sistema descentralizado e interoperable para la comunicación transfronteriza para facilitar el intercambio electrónico de datos, en particular cualquier contenido transmisible en formato electrónico, de manera rápida, segura y fiable en el ámbito de la cooperación judicial en materia civil y penal.

[56] Considerando n. 9 del Reglamento (UE) 2023/2131.

[57] Art. 85 TFUE y considerando n. 25 del Reglamento (UE) 2023/2131.

[58] Considerando n. 10 del Reglamento (UE) 2023/2131.

[59] Ídem.

[60] En septiembre de 2019, sobre la base de la Decisión 2005/671/JAI del Consejo de 20 de septiembre de 2005 relativa al intercambio de información y a la cooperación sobre delitos de terrorismo, OJ L 253, 29.9.2005, Eurojust creó el Registro Judicial Antiterrorista europeo a fin de identificar nexos entre procedimientos judiciales contra sospechosos de delitos de terrorismo y las consiguientes necesidades de coordinación. Eurojust 2019.

estructura, no permitiendo un intercambio cruzado de datos. Se necesitaba, por lo tanto, mejorar la capacidad de Eurojust para detectar vínculos y comparar datos biométricos, puesto que la transmisión de datos estructurados reduce las cargas administrativas y la calidad de los resultados de cotejo de la información[61].

La nueva infraestructura digital integrará el CTR, trasmitiéndole información, para que pueda almacenar datos y realizar el intercambio cruzado de información relativa a investigaciones y procesos penales pendientes contra personas sospechosas de terrorismo[62]. La detección de tales vínculos entre investigaciones sobre terrorismo y procedimientos penales y la conservación de estos datos por Eurojust es fundamental.

En estos casos, los datos biométricos representan el único nexo con estas personas, pues en muchas ocasiones los nacionales de terceros países usan identidades falsas o dobles[63]. Por ello, su transmisión es determinante, aunque por supuesto con las debidas cautelas para no vulnerar el derecho a la vida privada y familiar y a los datos personales (art. 7 y 8 de la Carta), y solo con el objetivo de identificar a las personas implicadas en procesos penales sobre delitos de terrorismo.

Las autoridades nacionales competentes tienen la obligación de compartir la información con Eurojust lo antes posible y procurar actualizar el sistema, salvo en la fase procesal más temprana, cuando pueda comprometer investigaciones en curso o la seguridad de una persona o cuando sea contrario a intereses esenciales de la seguridad del Estado miembro afectado[64].

De tal forma, se pretende alcanzar los siguientes objetivos[65]:

> "a. apoyar la gestión y la coordinación de las investigaciones e instrucciones en procesos penales en las que Eurojust presta asistencia;
> b. garantizar el acceso seguro y el intercambio de información sobre las investigaciones e instrucciones en procesos penales en curso;
> c. permitir el cotejo de la información y la detección de vínculos;
> d. permitir la extracción de datos con fines operativos y estadísticos;
> e. facilitar la supervisión para garantizar que el tratamiento de los datos personales operativos es lícito y cumple el presente Reglamento y las normas aplicables en materia de protección de datos".

La comunicación digital segura y el intercambio de datos entre las autoridades nacionales y competentes y Eurojust se realizará a través del sistema

[61] Considerando n. 22 del Reglamento (UE) 2023/2131.
[62] Art. 23 del Reglamento (UE) 2023/2131.
[63] Considerando n. 13 del Reglamento (UE) 2023/2131.
[64] Considerando n. 17 del Reglamento (UE) 2023/2131.
[65] Art. 23 del Reglamento (UE) 2023/2131.

informático descentralizado[66]. El sistema de gestión de casos estará conectado a una red de sistemas informáticos y puntos de acceso e-Codex interoperables, que funcionan bajo la responsabilidad y la gestión individuales de cada Estado miembro y Eurojust para permitir un intercambio transfronterizo de información seguro y fiable. Cuando no sea posible por la indisponibilidad del sistema informático descentralizado o por circunstancias excepcionales, se realizará por el medio alternativo más rápido y adecuado, asegurando su fiabilidad y que ofrezca un grado equivalente de seguridad y protección de datos.

Las autoridades nacionales competentes trasmitirán a Eurojust la información de modo semiautomatizado y estructurado[67], atendiendo a lo previsto en el acto de ejecución, que adoptará la Comisión. Esta se encargará además de la creación, el mantenimiento y el desarrollo de un programa informático de aplicación de referencia que los Estados miembros y Eurojust pueden decidir utilizar como sistema dorsal (*back-end*), que se empaqueta y se entrega separado de los componentes e-CODEX necesarios para conectarlo al sistema informático descentralizado. Dicha configuración permitirá a los Estados miembros reutilizar o mejorar sus infraestructuras nacionales existentes de comunicación judicial con fines de uso transfronterizo y hacer posible que Eurojust conecte su sistema de gestión de casos al sistema informático descentralizado.

El nuevo sistema sustituirá progresivamente el anterior, formado por ficheros temporales de trabajo y un índice, a través del que los miembros nacionales de Eurojust intercambian la información pertinente. Ahora bien, ante la complejidad del proceso de migración de los datos, que ha impedido a Eurojust respetar el plazo previsto del 1º de diciembre 2025 para activar el nuevo sistema, el Reglamento 2025/2082 ha previsto un periodo transitorio en el que los dos sistemas tendrán que compaginarse, permitiendo utilizar ambos sistemas de gestión de casos hasta el 1º de diciembre de 2027[68].

De esta forma, se ha concedido a Eurojust el margen necesario para la puesta en marcha del nuevo sistema de gestión de casos, reduciendo a la vez el periodo de tiempo en el que es posible duplicar de forma excepcional datos personales operativos. También el Supervisor Europeo de Protección de Datos, en el desempeño de su función consultiva, ha avalado en el dictamen 6/2025, de 22 de abril de 2025, el funcionamiento "paralelo" del "antiguo" y

[66] Art. 22 bis del Reglamento (UE) 2023/2131.

[67] Art. 21 y 21 bis del Reglamento (UE) 2023/2131.

[68] Reglamento (UE) 2025/2082 del Parlamento Europeo y del Consejo de 8 de octubre de 2025 por el que se modifica el Reglamento (UE) 2018/1727 en lo que respecta a la prórroga del plazo para el establecimiento del sistema de gestión de casos de Eurojust, DOUE, n. 2082, de 15 de octubre de 2025.

del "nuevo" sistema durante el periodo provisional de prórroga establecido, que concede dos años más para asegurar una "transición de éxito"[69].

Por lo tanto, atendiendo a la nueva formulación del art. 80, ap. 9, del Reglamento (UE) 2018/1727, tal y como ha sido previsto por el Reglamento 2025/2082, Eurojust podrá seguir utilizando el sistema anterior "hasta el 1 de diciembre de 2027, a menos que ya se haya implantado el nuevo sistema de gestión de casos y que se haya completado antes de dicha fecha la migración de los datos del sistema de gestión de casos compuesto por ficheros temporales de trabajo y un índice, así como la verificación de la exactitud de esos datos". Dicha medida se aplica a todos los Estados miembros, menos a Irlanda y Dinamarca[70], confirmando una vez más el enfoque asimétrico de la cooperación judicial en materia penal en la Unión.

4. La digitalización de la cooperación judicial transfronteriza en asuntos civiles, mercantiles y penales a través de e-Codex

En esta línea, el Reglamento (UE) 2023/2844[71] y la Directiva (UE) 2023/2843[72] sobre digitalización de la cooperación judicial transfronteriza en asuntos civiles, mercantiles y penales en la UE pretenden crear un "modelo armonizado"[73], basado en un "marco jurídico uniforme para el uso de la comunicación electrónica"[74], es decir "el intercambio digital de información por medio de internet o de otra red"[75], entre las autoridades competentes en dichos proce-

[69] European Data Protection Supervisor (EDPS) 2025.

[70] *Vid.* artículos 1 y 2, y 4 bis, ap. 1, del Protocolo n. 21; y artículos 1 y 2 del Protocolo n. 22.

[71] Reglamento (UE) 2023/2844 de 13 de diciembre de 2023 sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales, y por el que se modifican determinados actos jurídicos en el ámbito de la cooperación judicial, OJ, 2844, 27, 12.2023. La nueva normativa incide en numerosos actos jurídicos. Con respecto a los actos en el ámbito de la cooperación judicial en materia penal *vid.* el anexo II.

[72] Directiva (UE) 2023/2843 de 13 de diciembre de 2023 por la que se modifican las Directivas 2011/99/UE y 2014/41/UE, la Directiva 2003/8/CE y las Decisiones Marco 2002/584/JAI, 2003/577/JAI, 2005/214/JAI, 2006/783/JAI, 2008/909/JAI, 2008/947/JAI, 2009/829/JAI y 2009/948/JAI, en lo que respecta a la digitalización de la cooperación judicial, OJ L, 2023/2843, 27.12.2023. De forma análoga al Reglamento, también la Directiva sobre digitalización de la cooperación judicial ha modificado una serie de actos en materia penal para adaptarlos al contexto digital y concretar los cambios introducidos por el Reglamento para uniformar la normativa en dicho ámbito y dotarla de más seguridad jurídica.

[73] El considerando n. 58 del Reglamento (UE) 2023/2844 usa la expresión "digitalización armonizada de la cooperación judicial transfronteriza". Sobre estas medidas v. Gascón Inchausti 2024, 535-552; Fierro Rodríguez 2025.

[74] Art. 1 del Reglamento (UE) 2023/2844.

[75] Art. 2, par. 2, del Reglamento (UE) 2023/2844.

dimientos y entre personas físicas o jurídicas y autoridades competentes en procedimientos judiciales en materia civil y mercantil[76].

De tal forma, la UE intenta dar concreción a los principios de protección de datos desde el diseño y de "digital por defecto"[77], que incluye la información legible de forma automatizada, a fin de ofrecer servicios de carácter preferente en forma digital, aunque manteniendo abiertos otros canales, para quienes no puedan o no quieran conectarse. También en este caso se han adherido a esta medida todos los Estados menos Irlanda y Dinamarca.

La modernización de la normativa sobre procedimientos transfronterizos en la UE, mediante la digitalización de los canales de comunicación, dota al sistema de un plus de eficiencia y de efectividad, pretende facilitar el acceso a la justicia, reducir la carga administrativa y los tiempos de tramitación y asegurar una mayor capacidad de reacción para las autoridades ante causas de fuerza mayor. Tales aspectos positivos pueden contribuir a reforzar la estrategia de la UE en la lucha contra asuntos transfronterizos de carácter penal, garantizando un elevado nivel de seguridad y una mayor protección de los derechos de las personas involucradas, favoreciendo también la ejecución de los instrumentos de reconocimiento mutuo.

A tal fin, se instituirá "una red de sistemas informáticos y puntos de acceso interoperables", bajo la responsabilidad y la gestión individuales de cada Estado miembro, órgano u organismo de la Unión[78]. Sus puntos de acceso se basarán en e-Codex[79], que se convierte en el centro de imputación de este sistema descentralizado, habiendo asumido eu-LISA también la responsabilidad de este sistema.

El uso de un sistema informático descentralizado, cuyo objetivo es garantizar un intercambio de datos seguro y autónomo entre las autoridades nacionales y los organismos de la UE involucrados, es obligatorio, salvo cuando sea imposible por una interrupción del sistema, o por las características de la información, como en el caso de pruebas materiales, o se necesite analizar un documento original en papel para comprobar su autenticidad o por situaciones de fuerza mayor[80]. En estos supuestos, se deberá elegir el medio de comunicación alternativo más adecuado en términos de rapidez y seguridad

[76] Art. 1 del Reglamento (UE) 2023/2844.

[77] Considerando n. 1 del Reglamento (UE) 2023/2844. Según la Estrategia para un Mercado Digital para Europa relativa al Plan de Acción de administración electrónica de la UE 2016 — 2020 — Acelerando la transformación digital de la administración, Bruselas, 19.4.2016, COM (2016) 179 final, los principios fundamentales en este ámbito son: digital por defecto, principio de solo una vez, inclusión y accesibilidad, apertura y transparencia, transfronterizo de forma predeterminada, interoperabilidad de forma predeterminada, confianza y seguridad.

[78] Art. 2.3 del Reglamento (UE) 2023/2844.

[79] Considerando n. 20 del Reglamento (UE) 2023/2844.

[80] Considerando n. 24 del Reglamento (UE) 2023/2844.

como por servicio postal o trasmisión en persona. Asimismo, puede haber situaciones en las que las autoridades necesiten una comunicación personal directa[81], menos formal, como a través del correo electrónico, u otros medios de comunicación por la necesidad de tratar datos particularmente delicados[82].

En el art. 6 del Reglamento (UE) 2023/2844 se prevé una regulación específica para las vistas orales en los procedimientos transfronterizos de carácter penal, reconociendo el uso facultativo de la videoconferencia u otras tecnologías de comunicación a distancia, a fin de comprobar la identidad de la persona, que tiene que declarar y facilitar la comunicación audiovisual, sonora y oral durante la vista[83]. Entran en el ámbito de aplicación de dicha normativa los procedimientos relativos a la ejecución de una orden europea de detención[84] y de una orden europea de protección[85], al reconocimiento mutuo de sentencias en materia penal por las que se imponen penas u otras medidas privativas de libertad[86], de libertad vigilada con miras a la vigilancia de las medidas de libertad vigilada y las penas sustitutivas[87], de las medidas de vigilancia como sustitución de la prisión provisional[88] y de las resoluciones de embargo[89].

El procedimiento respetará el Derecho del Estado miembro en el que se realice este trámite y que haya solicitado el uso de tecnologías de comunicación a distancia[90]. El presente Reglamento no se aplica al uso de la videocon-

[81] Considerando n. 25 del Reglamento (UE) 2023/2844.

[82] Art. 3 del Reglamento (UE) 2023/2844.

[83] Considerando nn. 31 y 32 y art. 6 del Reglamento (UE) 2023/2844.

[84] Decisión Marco del Consejo 2002/584/JAI de 13 de junio de 2002 relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, DO L 190, 18.7.2002.

[85] Directiva 2011/99/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011 sobre la orden europea de protección, DO L 338, 21.12.2011, en particular art. 6, ap. 4.

[86] Decisión Marco 2008/909/JAI del Consejo de 27 de noviembre de 2008 relativa a la aplicación del principio de reconocimiento mutuo de sentencias en materia penal por las que se imponen penas u otras medidas privativas de libertad a efectos de su ejecución en la Unión Europea, DO L 327, 5.12.2008, en particular el art. 6, ap. 3.

[87] Decisión Marco 2008/947/JAI del Consejo de 27 de noviembre de 2008 relativa a la aplicación del principio de reconocimiento mutuo de sentencias y resoluciones de libertad vigilada con miras a la vigilancia de las medidas de libertad vigilada y las penas sustitutivas, DO L 337, 16.12.2008, en particular el art. 17, ap. 4.

[88] Decisión marco 2009/829/JAI del Consejo de 23 de octubre de 2009 relativa a la aplicación, entre Estados miembros de la Unión Europea, del principio de reconocimiento mutuo a las resoluciones sobre medidas de vigilancia como sustitución de la prisión provisional, DO L 294, 11.11.2009, en particular art. 19, ap. 4.

[89] Reglamento (UE) 2018/1805 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso, PE/38/2018/REV/1, DO L 303, 2018.

[90] Considerando n. 42 del Reglamento (UE) 2023/2844; y art. 6 del Reglamento (UE) 2023/2844 sobre las vistas por videoconferencia o por medio de otras tecnologías de comunicación a

ferencia o de otras tecnologías de comunicación a distancia para conseguir pruebas o celebrar un juicio, que pueda dar lugar a una resolución sobre la culpabilidad o la inocencia de un sospechoso o de un acusado[91]. En este sentido, la posibilidad de recurrir a estas herramientas digitales se considera por defecto, siendo posible cuando lo justifiquen las circunstancias concretas del asunto.

En cuanto al consentimiento, que constituye la regla general, su obtención puede ser excepcionada en circunstancias extraordinarias, en las que se produzca una amenaza grave para la seguridad y la salud públicas reales y presentes o previsibles[92]. Todo ello, evidentemente, sin perjuicio de la imparcialidad del proceso y del derecho a la tutela judicial efectiva en virtud del Derecho procesal nacional. Al margen de dichas situaciones excepcionales, el presente Reglamento rodea el requisito del consentimiento de una serie de garantías. Se prevé que tendrá que ser voluntario e inequívoco, correspondiéndole a la autoridad competente requirente verificarlo antes de la vista y dejar constancia de ello en los registros correspondientes[93].

Además, antes de manifestar su voluntad en este sentido, el interesado puede solicitar asistencia letrada y las autoridades procurarán facilitarle la información sobre el procedimiento en cuestión y sus derechos procesales, con la inclusión del derecho a recibir asistencia de un interprete y de un letrado. Y en esta línea garantista, se reconoce el carácter confidencial de las comunicaciones antes y durante la vista entre la persona sospechosa, acusada, condenada o afectada y su abogado, de conformidad con el Derecho nacional aplicable[94]. Se establecen particulares cautelas en el caso de que quien tenga que declarar sea un menor, correspondiéndole a las autoridades informar a los titulares de la patria potestad u otro adulto adecuado antes de dicho trámite[95], siempre y cuando se considere apropiado para satisfacer el interés superior del menor[96].

Asimismo, es interesante observar que se extiende el marco relativo a las vistas realizadas por videoconferencia u otras tecnologías de comunicación a distancia en asuntos transfronterizos a asuntos internos, cuando el "Derecho nacional de un Estado miembro disponga la grabación de vistas para asuntos internos", correspondiéndole al Estado miembro requirente estable-

distancia en materia penal.

[91] Considerando n. 43 del Reglamento (UE) 2023/2844.

[92] Considerando n. 44 del Reglamento (UE) 2023/2844.

[93] Art. 6.2 del Reglamento (UE) 2023/2844.

[94] Art. 6, par. 5, del Reglamento (UE) 2023/2844.

[95] Art. 3, ap. 2, y art. 5, ap. 2, de la Directiva (UE) 2016/800 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 relativa a las garantías procesales de los menores sospechosos o acusados en los procesos penales, DO L 132, 21.5.2016.

[96] Art. 6, par. 6, del Reglamento (UE) 2023/2844.

cer a nivel interno las garantías adecuadas para que dichas grabaciones sean realizadas y almacenadas de forma segura y no sean difusas públicamente.

Y, por último, se reconoce el derecho a solicitar el reexamen, atendiendo a lo dispuesto en el Derecho nacional, cuando no se solicite el consentimiento, y en general no se respeten las garantías previstas. Todo ello sin perjuicio ante eventuales violaciones de derechos fundamentales de los afectados de asegurar el derecho a la tutela judicial efectiva (art. 47 de la Carta)[97].

En definitiva, estamos ante un sistema sin duda muy ambicioso, que plantea retos importantes, aunque no está exentos de riesgos, al tensionar y poner en entredicho postulados fundamentales del ordenamiento, que pueden verse lesionados en la aplicación práctica, desde la igualdad a exigencias estructurales como la independencia judicial, y con ello la separación de poderes y todos los demás principios, que se pueden reconducir en el concepto de Estado de Derecho (art. 2 TUE), *in primis* el respeto de los derechos procesales básicos.

Ahora bien, este nuevo sistema, para que pueda funcionar realmente y cumplir con sus objetivos, tiene que ser inclusivo en la práctica, asegurando el "acceso a la justicia para todos"[98]. De lo contrario, acabaría siendo disfuncional y discriminatorio, puesto que la eficiencia en el intercambio electrónico de datos no puede llevar a apartar determinadas categorías de personas, particularmente vulnerables, como las personas con discapacidad o con acceso limitado a las tecnologías, por falta de competencias, también por razones económicas, impidiéndoles el ejercicio de sus derechos fundamentales[99].

Esto conlleva por parte de las autoridades competentes una serie de tareas, sin duda no sencillas, que van del deber de concienciar a la ciudadanía europea sobre las ventajas que pueden derivar de este nuevo sistema, predisponiendo en su caso herramientas de auxilio, al deber de formación de los operadores jurídicos, como los fiscales, los jueces y el personal administrativo y en general las autoridades competentes, para que aprendan a usar el sistema informático descentralizado, la videoconferencia u otras tecnologías de comunicación a distancia[100], y de disponer de una infraestructura tecno-

[97] Art. 47 de la Carta y considerando n. 45 del del Reglamento (UE) 2023/2844.

[98] Considerando n. 10 del Reglamento (UE) 2023/2844.

[99] Al respecto, el art. 6, par. 3, del Reglamento (UE) 2023/2844, hace referencia expresa a las personas con discapacidad, estableciendo que "La autoridad competente requerida garantizará que las personas a que se refiere el apartado 2, en particular aquellas con discapacidad, tengan acceso a la infraestructura necesaria para realizar una videoconferencia o emplear otras tecnologías de comunicación a distancia".

[100] Art. 11 del Reglamento (UE) 2023/2844.

lógica adecuada[101], a fin de asegurar el acceso y una interactuación segura, eficiente, rápida, interoperable, confidencial y fiable[102].

5. El sistema Prüm II como respuesta a la libre circulación de criminales a través de la libre circulación de los datos

El Reglamento Prüm II, adoptado en marzo de 2024 (Reglamento (UE) 2024/982), relativo a la búsqueda y al intercambio automatizado de datos para la cooperación policial[103], modifica el sistema anterior. De esta forma, se refuerza el enfoque de seguridad y, con ello, el rol tanto de los Estados miembros como de Europol, cuyo punto de enlace está representado por eu-LISA. Estamos ante un ejemplo muy interesante, pero a la vez inquietante, de cómo el intercambio de datos a través de la digitalización está trasformando la forma de comunicar y llevar a cabo las actividades de *law enforcement* y la cooperación[104] para identificar a las personas involucradas en la comisión de un delito con elementos trasnacionales. También en este caso esta medida no se aplica ni a Irlanda ni a Dinamarca.

El nuevo sistema es sin duda oportuno. Es suficiente pensar que el alcance extraterritorial de la delincuencia crea vinculos entre lugares distintos y el autor del crimen, desarrollando un espacio de libre circulacion de los criminales, al que hay que responder con la libre circulacion de los datos de estas personas entre las autoridades competentes en la investigación, detección y enjuiciamiento del crimen, que también deberían moverse en un espacio sin fronteras. Atendiendo a los datos, en "2021, se comprobó que más del 70 % de las organizaciones delictivas tenían presencia en más de tres Estados miembros"[105].

En dicho marco, el Reglamento Prüm II junto a la Directiva sobre intercambio de informaciones entre autoridades judiciales de los Estados miembros[106] intende suplir las deficiencias del sistema actual en relación con la falta de comunicación directa en el intercambio de datos, la existencia de lagunas, la falta de armonización y de cumplimiento de la normativa por parte de

[101] Considerando n. 47 del Reglamento (UE) 2023/2844.
[102] Considerando n. 19 del Reglamento (UE) 2023/2844.
[103] Reglamento (UE) 2024/982 de 13 de marzo de 2024 relativo a la búsqueda y al intercambio automatizados de datos para la cooperación policial, y por el que se modifican las Decisiones 2008/615/JAI y 2008/616/JAI del Consejo y los Reglamentos (UE) 2018/1726, (UE) 2019/817 y (UE) 2019/818 (Reglamento Prüm II), PE/75/2023/REV/1, DO L, 2024/982, 5.4.2024.
[104] Comisión Europea 2020.
[105] Europol 2021.
[106] Directiva (UE) 2023/977 de 10 de mayo de 2023 relativa al intercambio de información entre los servicios de seguridad y de aduanas de los Estados miembros, por la que se deroga la Decisión Marco 2006/960/JAI del Consejo, DOUE, n. 134, 22.5.2023.

determinados Estados Miembros, los cuales acaban beneficiando a los criminales[107].

El sistema de Prüm II se enamarca en la cooperacion policial. Sus bases normativas se encuentran en el art. 87.2 TFUE, siendo su finalidad facilitar el intercambio de datos personales entre las autoridades competentes, y el art. 88.2 TFUE sobre el rol de Europol en relación con el refuerzo de la seguridad interior. Tales preceptos, a su vez, tienen que ser ponderados con el derecho a la protección de datos personales, previsto en los artículos 16 TFUE, 8 CEDH y 7 de la Carta, que, con arreglo a la jurisprudencia del TJUE[108], no es concebido como un derecho absoluto, sino que debe considerarse atendiendo a su función en la sociedad, y la Directiva (UE) 2016/680[109]. La regulación por la UE de dichos aspectos no afecta a la competencia exclusiva de los Estados sobre sus propias bases de datos nacionales de ADN[110]. Y con respecto a la fuente, se ha optato por el reglamento por la necesidad de que esta normativa sea directa y uniformemente aplicable en todos los Estados miembros.

De esta forma, por un lado, los Estados miembros podrán comprobar de forma automática los datos biométricos procedentes de terceros países conservados por Europol y ponerlos a disposición de las autoridades policiales. Por otro, Europol, que será parte integrante del marco de Prüm, podrá cotejar los datos procedentes de terceros países sobre delincuentes y terroristas, con la inclusión de los que se encuentran en las bases de datos nacionales de los Estados miembros, estableciendo vínculos[111].

Más en concreto, se regulan los "procedimientos de búsqueda automatizada de perfiles de ADN, datos dactiloscópicos, determinados datos de matriculación de vehículos, imágenes faciales y antecedentes policiales"[112] para permitir el intercambio de información entre las autoridades de *law enforcement* sobre personas involucradas en el proceso penal en cuanto sospechosas y acusadas y o incluso desaparecidas en el contexto de investigaciones penales o por motivos humanitarios y la identificación de restos humanos.

[107] Comisión Europea, 2021.

[108] Entre otras, v. STJUE, de 26.10.23, *FT y DW*, C-307/22.

[109] Directiva (UE) 2016/680 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.

[110] Considerando n. 12 del Reglamento (UE) 2024/982.

[111] Sobre el rol de Europol tras la reforma de 2022, v. Faggiani 2024; Tassinari 2024.

[112] Considerando n. 8 del Reglamento (UE) 2024/982.

A tales efectos, el enrutador Prüm II y EPRIS (Sistema Europeo de Índice de Antecedentes Policiales)[113] funcionarán como puntos de conexión entre los Estados miembros para que, accediendo a este sistema de intermediación, puedan comunicar entre sí. EPRIS responde al principio de protección de la intimidad desde el diseño, del que la seudonimización representa una de las principales garantías, puesto que los índices y las consultas no contienen datos personales legibles, sino cadenas alfanuméricas. El sistema no afectará al ECRIS. Además, se incorporan también los datos de personas procedentes de terceros países y conservados por Europol para ponerlos a disposición de los Estados miembros[114].

Se asiste a un sistema con un enfoque hibrido, entre descentralizado y centralizado, sin almacenamiento de datos a nivel central. Esto significa que no existirá una unica plataforma europea, sino que los Estados seguirán controlando sus propias plataformas nacionales, que se conectarán entre ellas, a través del router, al que pueden pedir informaciones sobre un determinado sujeto y que este router intentará recabar de los demás Estados miembros. La participación en estos procedimientos y el intercambio automatizado de antecedentes policiales son voluntarios y respetan el principio de reciprocidad.

Además, para la búsqueda automatizada de datos de matriculación de vehículos, los Estados miembros y Europol deben utilizar el sistema europeo de información sobre vehículos y permisos de conducción EUCARIS, cuya naturaleza es intergubernamental, conectando a todos los Estados miembros participantes a través de una red. En este caso, la comunicación no se realiza a través de un elemento centralizador, sino que cada Estado miembro puede comunicarse con los demás Estados miembros conectados y con Europol[115]. En todo esto, eu-LISA recibirá información por parte de los Estados miembros sobre las capacidades de búsqueda de datos dactiloscópicos[116] y sobre cualquier indisponibilidad del intercambio automatizado de datos, a fin de poner en marcha medidas alternativas, y llevará un registro de todas las operaciones de tratamiento de datos realizadas a través del enrutador[117].

Los datos recibidos serán procesados por un Estado miembro o por Europol solo para los fines del Reglamento, salvo previa autorización del Estado que haya proporcionado los datos[118]. Tras haber obtenido la respuesta automatizada a la búsqueda, dichos datos se suprimirán inmediatamente, a menos que se necesite un tratamiento ulterior o previa autorización. Además, serán

[113] Art. 42 del Reglamento (UE) 2024/982.
[114] Considerandos nn. 18 y 19 del Reglamento (UE) 2024/982.
[115] Considerando n. 15 del Reglamento (UE) 2024/982.
[116] Art. 14 del Reglamento (UE) 2024/982.
[117] Artículos 40 y 41 del Reglamento (UE) 2024/982.
[118] Art. 50 del Reglamento (UE) 2024/982.

marcados en el caso de que el interesado recurra la exactitud de las informaciones, de las que disponga un Estado miembro o de Europol o cuando estos no puedan asegurar la exactitud. Los Estados miembros o Europol pueden eliminarlos previo consentimiento del interesado o con arreglo a la decisión del juez competente, de la autoridad de control o del SEPD.

El tratamiento de datos y la adopción de las medidas necesarias en relación con el enrutador le corresponderá a eu-LISA y Europol se ocupará de los datos personales a través del EPRIS[119]. Las autoridades competentes de los Estados miembros, eu-LISA y Europol tienen que asegurar la seguridad del tratamiento, cooperando y adoptando las medidas necesarias para proteger los datos físicamente, impidiendo el acceso, la consulta o la introducción de datos a personas no autorizadas[120].

Si se produjera un incidente de seguridad, que afecte al enrutador, cooperarán entre sí para garantizar una respuesta. Eu-LISA notificará cualquier problema, que surja al Servicio de Ciberseguridad de las instituciones, órganos y organismos de la Unión (CERT-EU). Los Estados establecerán sanciones efectivas, proporcionadas y disuasoria para responder a un uso indebido de datos, tratamiento o intercambio. La responsabilidad derivada del incumplimiento de las obligaciones les incumbirá al Estado en cuestión o a Europol, salvo que estos hayan adoptado las medidas adecuadas para impedir que esto ocurrirá o para atenuar sus efectos[121].

El SEPD, al menos cada cuatro años, llevará a cabo una auditoría de las operaciones relativas al tratamiento de datos personales procesados por eu-LISA y Europol, cuyos resultados serán recogidos en un informe para el Parlamento Europeo, el Consejo, la Comisión, los Estados miembros y la agencia de la Unión interesada[122]. Eu-LISA y Europol pueden formular comentarios antes de la aprobación de los informes.

Por último, por lo que se refiere a las responsabilidades, la estructura central durante la fase de diseño y desarrollo del enrutador y de las adaptaciones técnicas estará alojada en eu-LISA[123]. El Consejo de Administración de eu-LISA aprobará el diseño, previo dictamen favorable de la Comisión. El Consejo de Administración del Programa presentará mensualmente al Consejo de Administración de eu-LISA informes escritos sobre los avances. No obstante, no tendrá competencia para adoptar decisiones, ni mandato alguno para representar a los miembros del Consejo de Administración de eu-LISA. El grupo consultivo de interoperabilidad se reunirá periódicamente hasta

[119] Art. 52 del Reglamento (UE) 2024/982.
[120] Art. 53 del Reglamento (UE) 2024/982.
[121] Artículos 54-57 del Reglamento (UE) 2024/982.
[122] Art. 58 del Reglamento (UE) 2024/982.
[123] Art. 66 del Reglamento (UE) 2024/982.

que el enrutador entre en funcionamiento. Presentará un informe al Consejo de Administración del Programa después de cada una de sus reuniones, aportará los conocimientos técnicos necesarios para apoyarlo en sus tareas y realizará un seguimiento del estado de preparación de los Estados miembros. Y tras la entrada en funcionamiento del enrutador (art. 67), eu-LISA será responsable de la gestión técnica de la infraestructura central del enrutador, incluidos su mantenimiento y avances tecnológicos[124].

6. Conclusiones

La Unión Europea está adoptando medidas muy interesantes, que permitirán consolidar un modelo de cooperación judicial en materia penal y de cooperación policial digitalizado, de acuerdo con la Estrategia Europea sobre la Justicia en Red. El centro neurálgico de este sistema está representado por eu-LISA, la Agencia de la UE, que se encarga del alojamiento y de la gestión de los sistemas informáticos de gran magnitud en el ELSJ, y por la relación que esta ha conseguido desarrollar con las demás agencias con competencias en estos ámbitos, en particular Eurojust y Europol. Esta proficua colaboración, que se ha llevado a cabo antes en el plano operativo, desde la implementación de actos de *soft law*, buenas prácticas y protocolos, ha ido en los últimos años hacia a más, impulsando la adopción de actos legislativos, que han sido objeto de análisis en esta contribución.

Estos mecanismos, que buscan una mayor comunicación y trasmisión de informaciones entre las autoridades de los Estados miembros y también de los terceros Estados, pretenden reforzar la lucha contra la criminalidad organizada, dotando al sistema no solo de mayor eficacia sino sobre todo de mayor seguridad, que debe concebirse como una prioridad. En efecto, tal y como se afirma en la Estrategia Europea de Seguridad Interior ("ProtectEU"), "la seguridad sienta los cimientos sobre los que se levantan todas nuestras libertades. La democracia, el Estado de Derecho, los derechos fundamentales, el bienestar de los europeos, la competitividad y la prosperidad: todo ello depende de nuestra capacidad de ofrecer unas garantías básicas" para que los ciudadanos puedan circular libremente en un espacio seguro[125].

En dicho marco, las autoridades judiciales y policiales deben poder desempeñar su trabajo de detección del crimen, desmantelando las redes criminales y protegiendo a las víctimas del delito y, en definitiva, impartiendo justicia. Los crímenes cometidos a través del uso de la tecnología como "terrorismo, la delincuencia organizada, el fraude en línea, el tráfico de drogas, el abuso

[124] Art. 67 del Reglamento (UE) 2024/982.
[125] En este sentido, Comisión Europea 1.4.2025; y Comisión Europea, 24.6.2025.

sexual de menores, la extorsión sexual en la red, los programas de secuestro y numerosos otros delitos" suelen tener "una característica en común": "dejan rastros digitales"[126]. No obstante, por otra parte, las extraordinarias potencialidades de la digitalización para los criminales les permiten innovar su estrategia, eludiendo fácilmente la justicia. De ahí, la necesidad de responder a la interconexión de la criminalidad mediante una mayor interconexión entre las autoridades de la cooperación judicial.

Esta contribución se ha centrado en la plataforma de colaboración para los ECI y el "nuevo" sistema de gestión de casos de terrorismo de Eurojust, la digitalización de los instrumentos de comunicación en la cooperación judicial transfronteriza en asuntos civiles, mercantiles y penales y el sistema Prüm II, con el que se pretende dar respuesta a la libre circulación de criminales a través de la libre circulación y el intercambio automatizado de datos[127].

Ahora bien, este nivel elevado de tecnologización aumenta los riesgos derivados del uso de datos biometricos, los posibles errores y las discriminaciones por sesgos[128]. Y en este sentido, tenemos que leer el impacto del uso de datos de este tipo en relación con el Reglamento de la UE por el que se establecen normas armonizadas sobre la IA, el Reglamento (UE) 2024/1689, que prevé el uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de garantía del cumplimiento del Derecho, en la medida en que dicho uso sea estrictamente necesario para los objetivos de investigación y persecución de delitos, indicados en el art. 5, par. 1, h, para verificar la identidad de la persona[129]. La contrapartida del uso de una tecnología tan eficaz pero a la vez tan intrusiva es el desarrollo de una sociedad del control y de la vigilancia.

Por otra parte, además de los problemas derivados del carácter autárquico de la tecnología, que la hace incontrolable y muy invasiva en los derechos fundamentales, no se pueden soslayar las preocupaciones que despierta el proceso de agencificación, es decir, la delegación en las agencias de la UE de competencias para llevar a cabo las políticas de la EU. Las extraordinarias potencialidades de la gestión por parte de eu-LISA de los sistemas informáticos de gran magnitud, que se nutren de mecanismos basados en la IA y el importante rol, que asumen también las otras agencias del ELSJ, las cuales facilitarán sin duda las actividades de *law enforcement*, se ven matizadas por la opacidad de los procesos decisorios. En este sentido, dichas actividades suelen ser caracterizadas por la falta de transparencia, no existiendo instru-

[126] Comisión Europea, 24.6.2025; y Europol, 2025.
[127] Para una crítica a Prüm II, v. EDRI 6.2.2024.
[128] EDPS 2.3.2022.
[129] Escajedo San Epifanio 2014, 183-235.

mentos de control y rendición de cuentas realmente eficaces. Es suficiente pensar que los informes emitidos por dichos organismos y por la Comisión Europea siguen constituyendo mecanismos meramente políticos[130].

En definitiva, el que en el 80 % de los delitos se encuentran elementos digitales puede ser bastante indicativo de las proporciones de la dimensión tecnológica del crimen[131] y de la necesidad de responder a la digitalización de la criminalidad con la digitalización de la justicia. Estas cifras además están destinadas a seguir aumentando. Ahora bien, este afán por la modernización y la apuesta por la aplicación de la IA en aras de una supuesta eficacia y eficiencia[132] de los sistemas judiciales no puede ser a costa de los principios estructurales de nuestros ordenamientos. Aunque vivamos en un contexto fluido, caracterizado por cambios continuos, existen principios infranqueables (art. 2 TUE), que es necesario preservar porque de lo contrario se acabaría menoscabando el modelo de Estado constitucional de Derecho en su núcleo básico[133].

Bibliografía

Akbik, A., Freudlsperger, C., Migliorati, M. 2024. "Differentiated participation, uniform procedures: EU agencies in direct policy implementation". *West European Politics* 3: 645-670.

Alberti, J., 2018. *Le Agenzie dell'Unione europea.* Giuffrè.

Arangüena Fanego, C., De Hoyos Sancho, M., Pillado González, E. (dirs.) 2023. *El proceso penal ante una nueva realidad tecnológica europea.* Thomson Reuter Aranzadi.

Barbieri, D. 2007. "Agenzie Europee: un esempio di evoluzione (istituzionale) amministrativa?", *Rivista Italiana di Politiche Pubbliche* 3: 77-102.

Barona Vilar, S. 2017. "Justicia penal líquida (desde la mirada de Bauman)". *Teoría y derecho: revista de pensamiento jurídico* 22: 64-91.

Barona Vilar, S. 2022. "Mutación de la justicia en el siglo XXI. Elementos para una mirada poliédrica de la tutela de la ciudadanía", Barona Vilar, S., *Justicia poliédrica en período de mudanza: Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad*, 31-62. Tirant lo Blanch.

[130] Pacini 2018, 1053-1072.

[131] Comisión Europea 14.4.2021. Sobre las tendencias en este ámbito, v. también Europol 22.7.2024.

[132] Barona Vilar 2022, 31-62, habla del proceso de licuefacción del modelo de justicia penal o también de un proceso penal "líquido" o "liquidable", más célere, pero también menos garantista (ID 2017, 64-91).

[133] Brenner, M., y otros 2020, 267-310; Faggiani 2022, 517-546.

Brenner, M., y otros. 2020. "Constitutional Dimensions of Predictive Algorithms in Criminal Justice". *Harvard Civil Rights-Civil Liberties Law Review* 55 (1): 267-310.

Chiti, E. 2013. "'European Agencies' Rulemaking: Powers, Procedures and Assessment". *European Law Journal* 19 (1): 93-110.

Chiti, E. 2015. "Diritto amministrativo europeo, stabilizzazione dei comportamenti e costruzione dell'ordine sociale". *Diritto pubblico* 3: 909-984.

Comisión Europea. 24.7.2020. Comunicación sobre la Estrategia de la UE para una Unión de la Seguridad, Bruselas, COM(2020) 605 final.

Comisión Europea. 19.4.2016. Comunicación, el Plan de Acción de administración electrónica de la UE 2016 — 2020 — Acelerando la transformación digital de la administración, Bruselas, COM (2016) 179 final.

Comisión Europea. 24.6.2025. Comunicación, Hoja de ruta para un acceso lícito y efectivo a los datos por parte de las autoridades policiales y judiciales, COM(2025) 349 final.

Comisión Europea. 1.4.2025. Comunicación, ProtectEU: una Estrategia Europea para la Seguridad Interior Estrasburgo, COM(2025) 148 final.

Comisión Europea. 2.12.2020. Comunicación: "La digitalización de la justicia en la UE: Un abanico de oportunidades", COM/2020/710 final.

Comisión Europea. 14.4.2021. Comunicado de prensa: Lucha contra la delincuencia organizada: Nueva estrategia de cinco años para impulsar la cooperación en toda la UE y mejorar el uso de las herramientas digitales en las investigaciones, Bruselas.

Comisión Europea. 14.4.2021. Estrategia de la UE contra la Delincuencia Organizada 2021-2025, COM (2021) 170 final.

Consejo de la Unión Europea. 16.1.2025. Estrategia Europea relativa a la Justicia en Red 2024-2028, DOUE, C/2025/437.

Di Paolo, G. 2019. "Novità: Verso una nuova architettura di gestione dei dati contenuti nei sistemi di informazione dell'Unione". *Cassazione penale* 59 (9): 3380-3384.

EDRI. 6.2.2024. "Automated data exchange in Prüm II: The EU's securitisation mindset keeps encroaching on our fundamental rights". https://edri.org/our-work/automated-data-exchange-in-prum-ii-eu-securitisation-mindset-encroaching-on-fundamental-rights/.

Escajedo San Epifanio, L. 2024. "El reconocimiento biométrico en el reglamento de inteligencia artificial: Exenciones, prohibiciones y

especialidades de alto riesgo". En Cotino Hueso, L. y Simón Castellano, P. (dirs.), *Tratado sobre el reglamento de inteligencia artificial de la unión Europea.* Aranzadi la Ley: 183-235.

Eu-LISA e Eurojust. 22.7.2022. Joint Report: Artificial intelligence supporting cross-border cooperation in criminal justice. https://www.eurojust.europa.eu/publication/artificial-intelligence-supporting-cross-border-cooperation-criminal-justice.

Eurojust. 2022. EJ20 Anniversary essays, AI and data protection in judicial cooperation in criminal matters. https://www.eurojust.europa.eu/20-years-of-eurojust/ai-and-data-protection-judicial-cooperation-criminal-matters.

Eurojust. 20.6.2019. Press Release. Setting up of judicial counter-terrorism register at Eurojust. https://www.eurojust.europa.eu/news/setting-judicial-counter-terrorism-register-eurojust.

European Data Protection Supervisor. 16.4.2025. Opinion 6/2025 on the Proposal for a Regulation amending Eurojust Regulation as regards the extension of the timeframe for the establishment of the Eurojust case management system.

European Data Protection Supervisor. 2.3.2022. Opinion on the Commission's Proposal for the Regulation on automated data exchange for police cooperation ("Prüm II"). www.edps.europa.eu/system/files/2022-03/22-03-07_opinion-4-2022_prum_en.pdf.

Europol. 2025. Evaluación de la amenaza de la delincuencia grave y organizada de la Unión Europea para 2025. europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

Europol. 12.4.2021. Evaluación de la amenaza de la delincuencia grave y organizada de la UE de 2021, SOCTA. https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

Europol. 22.7.2024. Internet Organised Crime Threat Assessment (IOCTA) 2024. *https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024*, 22.7.2024.

Faggiani, V. 2022. "El derecho a un proceso con todas las garantías ante los cambios de paradigma de la inteligencia artificial". *Teoría y realidad constitucional* 50: 517-546.

Faggiani, V. 2021. "Eurojust en la lucha contra la criminalidad organizada". En Garrido Carrillo, F.J. (dir.), Faggiani, V. (coords.), *Retos en la lucha contra la delincuencia organizada. Un estudio multidisciplinar:*

garantías, instrumentos y control de los beneficios económicos, 185-210. Thomson Reuters Aranzadi.

Faggiani, V., 2024. "La Estrategia Europea sobre la Justicia Penal en Red: avances en la aplicación de la Inteligencia Artificial". *Derecho Digital e Innovación. Digital Law and Innovation Review* 19.

Fierro Rodríguez, D. (2025). "Perspectivas y expectativas ante los comienzos aplicativos del Reglamento (UE) 2023/2844, sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales". *Revista Derecho & Proceso.*

Gascón Inchausti, F. 2024. "The new regulation on the digitalisation of judicial cooperation in the European Union: something old, something new, something borrowed and something blue". *ERA Forum* 24: 535-552.

Illamola Dausà, M. 2015. "EU-LISA, el nuevo modelo de gestión operativa de las distintas bases de datos de la UE". *Revista CIDOB d'afers internacionals* 111: 105-126.

Pacini, M. 2018. "I regimi e la prassi di accountability di Europol ed Eurojust". *Rivista italiana di diritto pubblico comunitario* 28 (6): 1053-1072.

Pi Llorens, M. 2017. "El nuevo mapa de las agencias europeas del Espacio de Libertad, Seguridad y Justicia". *Revista de Derecho Comunitario Europeo* 21 (56): 77-117.

Signorin, S. 2025. "Verso l'applicazione trasversale del principio "digital by default" nel settore della cooperazione giudiziaria dell'Unione europea". *Rivista.eurojus.it* 1: 206-221.

Tassinari, F. 2024. "Issues of consistency and complementarity in EU privacy law: the europol's big data challenge". *Revista General de Derecho Europeo* 63: 133-169.

Tassinari, F. 2023. "La institucionalización de la competencia operativa de la Unión Europea para la gestión y la interoperabilidad de los sistemas informáticos de gran magnitud del Espacio de Libertad, Seguridad y Justicia: eu-LISA". *La Ley Unión Europea* 111.

Tassinari, F. 2022. "La interoperabilidad de los sistemas de información de gran magnitud de la Unión Europea y la detección de identidades múltiples: garantías y responsabilidades". En Garrido Carrillo, F.J. (dir.), Faggiani, V. (coord.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital*, 291-338. Thomson Reuters Aranzadi.

Torres Pérez, M. 2022. "Eurojust, veinte años de compromiso por la cooperación judicial penal en Europa. el futuro de la Agencia ante la guerra en Ucrania". *Revista Electrónica de Estudios Internacionales* 44: 1-17.