Rev Der Gen H, 60 - enero-diciembre 2024
https://doi.org/10.1387/rdgh.27359

Revista de Derecho y Genoma Humano
Law and the Human Genome Review
e-ISSN 2605-1230

Doctrina / Articles

El uso de los datos genéticos en la era del *big data:* Evolución y trayectorias futuras desde la óptica de Europol*

The use of genetic data in the era of Big Data: Evolution and future trajectories from Europol's perspective

Francesca Tassinari**
Investigadora postdoctoral Juan de la Cierva
Departamento de Derecho Público, Universidad del País Vasco / Euskal Herriko Unibertsitatea (UPV/EHU)
ResearcherID H-5751-2018
https://orcid.org/0000-0003-4487-7130

Palabras clave

Europol
big data
Interoperabilidad
Datos genético
Investigación e innovación

Resumen: El presente estudio analiza el papel de la Agencia de la Unión Europea (UE) para la Cooperación Policial (Europol) en la gestión y procesamiento de los datos genéticos para la lucha contra el crimen organizado y el terrorismo respaldados por la técnica del *big data*. Empieza resaltando como el entorno de la Tecnología Informática (TI) de Europol ha evolucionado desde su entrada en funcionamiento en el año 2001, momento clave en el que se desarrollaron el Sistema de Información de Europol (SIE) y la Aplicación de Red Segura para el Intercambio de Información (SIENA). De ahí que el Reglamento 2016/794 permite a esta Agencia procesar la información que ésta recaude (in)directamente de distintas fuentes para unas finalidades concretas, y en el respeto de los principios de la limitación del plazo de conservación y de la minimización de datos. No obstante, el desafío del *big data* denunciado por el Supervisor Europeo de Protección de Datos (SEPD) evidenció como las limitaciones impuestas a Europol para garantizar la protección de los datos personales procesados en su entorno obstaculizaban el análisis de grandes conjuntos de datos complejos (o macrodatos). Por consiguiente, el mandato de Europol ha sido revisado y, aunque haya pasado desapercibido, el art. 30 del Reglamento 2022/991, emendado, suprime la prohibición de procesar categorías especiales de datos personales. Dentro de estas categorías destacan los datos genéticos. La genética forense está beneficiándose de la revolución tecnológica impulsada por el *big data* gracias, sobre todo, al estudio del *Single Nucleotide Polymorphism* (SNP en inglés) que agiliza el análisis del fenotipo a partir del ácido desoxirribonucleico (ADN) no codificante. El estudio propuesto pone de relieve que el art. 33 bis del Reglamento Europol apodera la Agencia para procesar los datos genéticos a efectos de investigación e innovación. En concreto, se argumenta que el art. 33 bis del Reglamento Europol ampara la experimentación del aprendizaje automatizado basado en el *big data* a partir de los perfiles de ADN, más allá de la identificación de dubitados e indubitados desarrollada por la Agencia desde su origen.

* Esta publicación es parte de la ayuda JDC2022-048217-I, financiada por MCIN/AEI/10.13039/501100011033 y por la Unión Europea «NextGenerationEU/PRTR». La autora quiere agradecer al Grupo de Investigación del Sistema Universitario Vasco en Ciencias Sociales y Jurídicas aplicadas a las Nuevas Tecnologías (GI CISJANT, ref. IT1541-22), y al Prof. Iñigo de Miguel Beriain y a la Profa. Pilar Nicolás Jiménez, IPs del proyecto «Gobernanza de los usos secundarios de datos de salud y genéticos en espacios compartidos» (PID2022-137140OB-I00) concedido por la Agencia Estatal de Investigación española, por sus apreciaciones.

** ***Correspondencia a / Corresponding author:*** Francesca Tassinari. Investigadora postdoctoral Juan de la Cierva. Departamento de Derecho Público, Universidad del País Vasco (UPV/EHU) – francesca.tassinari@ehu.eus – https://orcid.org/0000-0003-4487-7130

Cómo citar / How to cite: Tassinari, Francesca (2024). «El uso de los datos genéticos en la era del *big data*: Evolución y trayectorias futuras desde la óptica de Europol», *Revista de Derecho y Genoma Humano*, 60, 17-54. (https://doi.org/10.1387/rdgh.27359).

e-ISSN 2605-1230 /

Keywords

Europol
Big Data
Interoperability
Genetic Data
Research and Innovation

Abstract: The present study analyzes the role of the European Union Agency for Law Enforcement Cooperation (Europol) in the management and processing of genetic data for combating organized crime and terrorism, supported by big data techniques. It begins by highlighting how Europol's Information Technology (IT) environment has evolved since its establishment in 2001, a key moment when the Europol Information System (EIS) and the Secure Information Exchange Network Application (SIENA) were developed. The 2016/794 Regulation allows this Agency to process information collected (in)directly from various sources for specific purposes, respecting the principles of data retention limitation and data minimization. However, the challenge posed by big data, as pointed out by the European Data Protection Supervisor (EDPS), demonstrated how the limitations imposed on Europol to ensure the protection of personal data processed in its environment hindered the analysis of large, complex data sets (or big data). Consequently, Europol's mandate has been revised, and, although it has gone unnoticed, Article 30 of the amended 2022/991 Regulation removes the prohibition on processing special categories of personal data. Among these categories, genetic data stand out. Forensic genetics is benefiting from the technological revolution driven by big data, especially through the study of Single Nucleotide Polymorphism (SNP), which accelerates phenotype analysis from non-coding deoxyribonucleic acid (DNA). The proposed study highlights that Article 33 bis of the Europol Regulation empowers the Agency to process genetic data for research and innovation purposes. Specifically, it argues that Article 33 bis of the Europol Regulation supports the experimentation of big data-based machine learning from DNA profiles, beyond the identification of questioned and known samples developed by the Agency since its inception.

1. Introducción

La Oficina Europea de Policía, hoy Agencia de la Unión Europea para la Cooperación Policial (Europol), surgió[1] del compromiso entre los Estados miembros[2] como agencia[3] de inteligencia determinada a recoger, compilar, transmitir y analizar información e inteligencia, incluso datos personales.[4] Aunque Europol haya ganado su parcela de poder sobre el terreno,[5] los Estados miembros han frenado la atribución de poderes coercitivos y han optado por potenciar su función de apoyo y coordinación. A tal efecto, el entorno informático de Europol ha ido evolucionando como centro neurálgico de información entre los Estados miembros para prevenir y luchar contra el terrorismo y la delincuencia grave y organizada, y velar sobre los intereses comunes en la Unión Europea (UE).[6] Europol ocupa, entonces, una posición privilegiada para detectar enlaces entre grandes conjuntos de datos procedentes de distintas fuentes, elaborar estrategias predictivas para el cálculo del riesgo, y experimentar nuevas técnicas informáticas de Inteligencia Artificial (IA) con fines de investigación forense.[7]

Las enmiendas aportadas al mandato de Europol por el Reglamento 2022/991[8] autorizan el procesamiento rápido y prolongado de grandes conjuntos de datos de distintas formas, estructurados o no, por medio del

---

1 En su forma embrionaria, Europol se denominó Unidad de Drogas de Europol (EDU).

2 Acto del Consejo, de 26 de julio de 1995, relativo al establecimiento del Convenio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol), DOUE C 316, 27.11.1995, disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:31995F1127(01) [última consulta el 20 de abril de 2024].

3 Alberti, Jacopo *Le agenzie dell'Unione Europea*, Giuffré Editore, Milano, 2018.

4 Santos Vara, Juan «Las consecuencias de la integración de Europol en el Derecho de la Unión Europea: comentario a la Decisión del Consejo 2009/371/JAI, de 6 de abril de 2009», *Revista General de Derecho Europeo*, n.º 20, 2010, pp. 2-24, p. 7.

5 Art. 88.2, let. b), de la Versión consolidada del Tratado de Funcionamiento de la Unión Europea, DOUE C 326 de 26.10.2012, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A12012E%2FTX [última consulta el 20 de abril de 2024] (TFUE en adelante) y Pi Llorens, Montserrat «El nuevo mapa de las agencias europeas del espacio de libertad, seguridad y justicia», *Revista de Derecho Comunitario Europeo*, n.º 56, 2017, pp. 77-117.

6 Art. 88 del Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007, DOUE C 306, 17.12.2007, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12007L%2FTXT [última consulta el 20 de abril de 2024].

7 Neiva, Laura «Big Data technologies in criminal investigations: The frames of the members of Judiciary Police in Portugal», *Criminology & Criminal Justice*, Vol. 0, n.º 0, 2023, pp. 1-23.

8 Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, de 8 de junio de 2022, por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innova-

análisis del *big data*[9] para agilizar la identificación de criminales y terroristas, así como experimentar el desarrollo, la formación, prueba y validación de los algoritmos útiles para la lucha contra la criminalidad y el terrorismo.[10] En efecto, los macrodatos[11] han asumido gran relevancia en el contexto policial[12] en aras de afinar el cribado masivo de perfiles genéticos, agilizar la formulación de correspondencias parciales entre perfiles y, en última instancia, inferir o predecir las características visibles de las personas (ojos, pelo, y pigmentación de la piel) mediante el análisis inteligente del *Single Nucleotide Polymorphism* (SNP en inglés).[13] A pesar de esto, existe una gran fragmentación entre los Estados a la hora de regular el análisis fenotípico. Delegar a la Agencia esta tarea permitiría, en última instancia, sortear la falta de armonización normativa entre los Estados miembros.[14] Además, con estas reformas, el legislador de la UE consigue reafirmar la posición privilegiada de Europol como eje de información policial por encima de sus Estados miembros.

El estudio propuesto rastrea la evolución del mandato de Europol para el análisis de los macrodatos con especial atención a la implementación del *big data* en la genética forense. Tomando reseña del desafío de los macrodatos denunciado ante el Supervisor Europeo de Protección de Datos (SEPD) por la propia Agencia, sobre el que ya se ha escrito,[15] analizaremos el uso del *big data*[16] a partir de las reformas aportadas

---

ción, DOUE L 169 de 27.6.2022, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R0991 [última consulta el 20 de abril de 2024].

9 Romeo Casabona, Carlos María «Revisión de las categorías jurídicas de la normativa europea ante la tecnología del *big data* aplicada a la salud», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext. 1, 2019, pp. 85-127, p. 89 y Valls Prieto, Javier *Problemas jurídicos penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*, Dykinson, Madrid, 2017, p. 20 y ss.

10 Europol Observatory Lab, *The Second Quantum Revolution – The impact of quantum computing and quantum technologies on law enforcement*, Luxemburgo, 2023, p. 13 y ss., disponible en: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing [última consulta el 17 de septiembre de 2024].

11 Tal y como señalan Alcalde Bezhold, Guillermo y Alfonso Farnós, Iciar «Utilización de tecnología *Big Data* en investigación clínica», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext., 2019, pp. 53-88, p. 56, existen muchas definiciones del término macrodatos (o *big data* en inglés); generalmente, el término *big data* designa a grandes volúmenes de información de distinta naturaleza cuyo análisis rápido deja vislumbrar información oculta o correlaciones imprevistas (las famosas tres «v» de volumen, variedad, y velocidad).

12 Merino Gómez, Gustavo «Nuevos desafíos en torno al big data», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext. 1, 2019, pp. 37-54 y Morente Parra, Vanessa «Big Data o el arte de realizar datos masivos. Una reflexión crítica desde los derechos fundamentales», *Derechos y libertades*, Vol. 2, n.º 4, 2019, pp. 225-260, p. 228.

13 Toom, Victor *Cross-Border Exchange and Comparison for Forensic DNA Data in the Context of the Prüm Decision*, Estudio para la Comisión LIBE, Bruselas, 2018, p. 23.

14 La Comisión Nacional para el Uso Forense del ADN, *Guía para el uso forense del ADN*, Ministerio de Justicia, Madrid, 2019, y Canales Serrano, Aurora «Forensic DNA phenotyping: A promising tool to aid forensic investigation. Current situation», *Spanish Journal of Legal Medicine*, Vol. 46, n.º 4, pp. 183-190, explican que el análisis fenotípico exige revisar la distinción jurídica entre ADN codificante y no codificante (distinción que aclararemos *infra*), y volver a abrir el debate ético-social sobre la creación de bases de datos de ADN centralizadas.

15 E.j., Drewer, Daniel y Miladinova, Vasela «The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation», *Computer Law & Security Review*, Vol. 3, n.º 33, 2017, pp. 298-308, disponible en: DOI:10.1016/j.clsr.2017.03.006 y Berthelet, Pierre «Europol face au défi de "mega-données": L'évolution tendancielle d'une coopération policière européenne "guidée par le renseignement"», *Revue du droit de l'Union Européenne*, n.º 2, 2019, pp. 157-187.

16 European Union Agency for Cybersecurity, *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*, Atenas, 17 de diciembre de 2015, disponible en: https://www.enisa.europa.eu/news/enisa-news/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics [última consulta el 13 de junio de 2024], que incluye en el término *big data* los macrodatos y su análisis para su el uso predictivo en los procesos decisionales, p. 12.

al entorno informático de Europol para (re)procesar[17] los datos personales en los límites de su mandato (punto 2.). A tal efecto, aclararemos a qué tipo de datos Europol puede acceder (punto 3.3.) y cómo, es decir, cuáles son las fuentes de información de Europol (punto 3.1) y para qué finalidades Europol puede procesar los datos personales y (eventualmente) usarlos ulteriormente (punto 3.2). Pasaremos luego a analizar la lenta integración de una protección legislativa reforzada para el tratamiento de las categorías especiales de datos personales en el mandato de Europol, incluidos los genéticos (punto 4.1). A tal efecto, avalaremos la hipótesis por la que ese régimen reforzado es aplicable a los perfiles de ADN de conformidad con el Reglamento de Protección de Datos Personales de la Unión Europea (RPDUE)[18] (punto 4.2). Finalmente, observaremos las finalidades por las que Europol puede analizar las categorías especiales de datos personales y, de forma más específica, los perfiles de ADN[19] (punto 4.3), haciendo hincapié en la experimentación algorítmica que Europol lleva a cabo en el marco de su (nueva) tarea de investigación e innovación (punto 4.3.2). En definitiva, este estudio destaca si Europol puede procesar y (eventualmente) reusar los datos personales con especial atención a los datos genéticos, así como las garantías que rodean, o deberían envolver, el procesamiento de esta categoría especial de datos personales a efectos, no tanto de identificación, sino de perfeccionamiento de los algoritmos como nueva herramienta de investigación policial.

2. Avances en la infraestructura informática del Sistema de Información de Europol

Para agilizar el intercambio de información, Europol ha sido dotado de una infraestructura informática, el Sistema de Información de Europol (SIE),[20] y una plataforma de comunicación denominada SIENA (Aplicación de Red Segura para el Intercambio de Información) desde el año 2001.[21] A partir del Reglamento 2016/794 ambas herramientas han sido actualizadas para soportar el procesamiento rápido de volúmenes ingentes de información.

Hasta el 2016, Europol podía procesar información en los Ficheros de Trabajo de Análisis (FTA), el Sistema de Índices (SI),[22] y otros sistemas de tratamiento de datos personales implantados en virtud de la decisión de su Consejo de Administración.[23] El Sistema de Análisis de Europol (EAS en inglés), por ejemplo, es un

---

17 De Montalvo Jääskeläinen, Federico «Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del Big Data», *UNED. Revista de Derecho Político*, n.º 106, pp. 43-75.

18 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE, DOUE L 295 de 21.11.2018, disponible en: https://eur-lex.europa.eu/eli/reg/2018/1725/oj?locale=es [última consulta el 20 de abril de 2024].

19 Los perfiles de ADN se extraen de las muestras biológicas cuyo tratamiento no está incluido en la definición de dato personal: cfr. Nicolás Jiménez, Pilar *La protección jurídica de los datos genéticos de carácter personal*, Comares, Granada, 2006, pp. 85 y ss. y la Organización Mundial de la Salud, *Draft Principles for human genome data access, use and sharing*, Ginebra, 8 de abril de 2024, punto 49, disponible en: https://cdn.who.int/media/docs/default-source/research-for-health/who-principles-human-genome-data-access--use--and-sharing_public-consultation_8-april.pdf?sfvrsn=f2c7afc7_3 [última consulta el 20 de abril de 2024].

20 Consejo de la UE, documento 8141/01, Bruselas, 24 de abril de 2001, p. 1.

21 Consejo de la UE, documento 9669/04, Bruselas, 24 de mayo de 2004.

22 Marica, Andrea *El sistema de tratamiento de la información de EUROPOL,* Working Paper n.º 309, Instituto de Ciencias Políticas y Sociales de la Universidad Autónoma de Barcelona, Barcelona, 2012.

23 La implantación de otros sistemas se ejecutó al amparo del art. 10.1 de la Decisión del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol), DOUE L 121 de 15 de mayo de 2009, disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32009D0371 [última consulta el 20 de abril de 2024].

sistema de información operativo alimentado con datos facilitados por los socios de Europol únicamente con fines analíticos, es decir, agencias de la Unión y terceros países u organizaciones internacionales con los que Europol había celebrado un acuerdo de cooperación o un acuerdo de trabajo. El mandato de Europol de 2016 ha incorporado el Concepto de Gestión Integrada de Datos (IDMC en inglés),[24] que se refiere a la interoperabilidad del tratamiento de diferentes conjuntos de datos —incluyendo el ADN y la información no genética— y establece un nuevo Sistema Automatizado de Identificación Dactilar (AFIS en inglés), una Solución de Reconocimiento Facial (FACE), y una mejor capacidad para procesar los perfiles de ADN. Europol ha abandonado el enfoque de compartimentos estancos entre sistemas y ha vertido sus repositorios en un único entorno operativo cuyo nombre se desconoce.[25] En el mismo año, Europol comenzó a diseñar el Nuevo Entorno Forense (NFE en inglés), que sustituiría a la Red Informática Forense (CFN en inglés), y mantiene el material forense disociado del análisis criminal de los perfiles.[26] En su conjunto, el NFE se mantendría separado del Repositorio de Herramientas de Europol (ETR en inglés), que a su vez es parte del Laboratorio de Innovación de Europol (EIL) dentro de la Unidad de Gestión de la Información (IMU en inglés) donde se realizan las actividades de prueba con fines de investigación e innovación, como explicaremos más adelante. Un entorno informático de este tipo permite a Europol desarrollar actividades de minería de datos, comprobaciones cruzadas (de forma sistemática o automatizada), vinculación y clasificación de información relacionada con delitos graves y terrorismo.[27] De esta forma, Europol puede suplir la falta de infraestructuras de alta tecnología de algunos Estados miembros y lograr capacidades forenses más avanzadas. Según el Consejo de la UE: «The new system […] will enable Europol to identify links and connections between different investigations and to detect emerging trends and patterns in organised crime (increased operational support capacity). Duplications are avoided as information can be cross-checked (flexibility and legal certainty)».[28]

La Aplicación de Red Segura para el Intercambio de Información (SIENA en inglés) funciona desde el año 2009 como sistema de mensajería electrónica segura de Europol y puede utilizarse de forma bilateral, entre los Estados miembros, entre Estados miembros y Europol, o entre socios de cooperación y Europol en cuyo caso la información se vierte en un entorno informático común a través del *Data Intake Utility* (DIU en inglés). A día de hoy, más de tres mil autoridades policiales de más de setenta países (Estados miembros de la UE y terceros países socios) y entidades internacionales están conectadas a SIENA. En 2023, el número de mensajes (traducidos de forma automática al inglés) intercambiados a través de SIENA alcanzó la cifra de uno con setenta y nueve millones, y se iniciaron más de ciento cincuenta y un mil casos a través de esta Red. Los ámbitos delictivos más señalados fueron el tráfico de drogas, el fraude y la inmigración ilegal. Sin embargo, el Tribunal de Cuentas criticó[29] a los Estados miembros por contribuir de forma diferente al entorno informático de Europol a causa de impedimentos operativos, organizativos y legales que desembocarían en imágenes situacionales poco fiables. De ahí que SIENA ha evolucionado, ampliando la comunidad de sus usuarios y convirtiéndose en una plataforma de acceso e intercambio de archivos de gran tamaño, como imágenes

---

[24] Neiva, Laura, Granja, Rafaela, y Machado, Helena «Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union», *Policing and Society*, Vol. 10, n.º 32, 2022, pp. 1167-1179.

[25] Comand-Kund, Florin «Europol's International Exchanges of Data and Interoperability of AFSJ Databases», *European Public Law*, Vol. 26, n.º 1, 2020, pp. 181-204.

[26] Cfr. García, Oscar y Alonso, Antonio «Las bases de datos de perfiles de ADN como instrumento en la investigación policial» Romeo Casabona, Carlos María (Ed) *Bases de datos de perfiles de ADN y criminalidad*, Comares, Granada, 2002, pp. 27-44.

[27] Carnevale, Stefania, Forlati, Serena y Giolo, Orsetta, *Redefining Organized Crime: A Challenge for the European Union,* Hart Publishing, Oxford, 2017, y Marrero Rocha, Inmaculada «Nuevas dinámicas en las relaciones entre crimen organizado y grupos terroristas», *Revista española de derecho internacional*, Vol. 69, n.º 2, 2017, pp. 145-169.

[28] Consejo de la UE, documento 14957/15 ADD 1, Bruselas, 24 de febrero de 2016.

[29] Tribunal de Cuentas, *EU information systems supporting border control - a strong tool, but more focus needed on timely and complete data*, Luxemburgo, 11 de noviembre de 2019, disponible en: https://www.eca.europa.eu/Lists/ECADocuments/SR19_20/SR_Border_control_EN.pdf [última consulta el 20 de abril de 2024].

forenses, extractos de dispositivos y grabaciones de vídeo y audio. Tras la COVID-19, SIENA ha pasado a ser accesible en cualquier momento, en cualquier lugar y con cualquier dispositivo y la Directiva sobre intercambio de información recientemente adoptada en sustitución del marco sueco obliga a los Estados miembros a utilizarla.[30] Aun así, Europol proporciona otras soluciones de comunicación para el intercambio de información bilateral entre Estados miembros. Es el caso, por ejemplo, del *Large File Exchange* (LFE en inglés), que intercambia grandes cantidades de datos más allá de la limitación de tamaño de SIENA y hasta cincuenta terabytes, o para archivos con una extensión no admitida por SIENA. Otros canales de comunicación suministrados por el entorno informático de Europol son la Plataforma de Expertos de Europol (PEE) para compartir información no personal,[31] los Expertos en Lucha Antiterrorista (ELA), el Núcleo de Delincuencia Internacional y Lucha Antiterrorista (CIC en inglés), la difusión de documentos de conocimiento a todos los Estados miembros (WIKIPOL en inglés), y los Grupos Operativos y de Tácticas Especiales (OTF en inglés).

La implementación de la técnica del *big data* en el nuevo entorno de Tecnología Informática (TI) permite a Europol procesar rápidamente un volumen cada vez más ingente de información, de distinta naturaleza, razón por la que el mandato adoptado en el año 2016 ha sido emendado, a pesar de las fuertes críticas recibidas.

3. Los límites competenciales de Europol para el análisis de los macrodatos

3.1. Las fuentes de información de Europol

Al margen de aquella información que Europol pueda generar por sí misma, el art. 17.1 del Reglamento Europol dispone cuales son las fuentes de información sobre las que Europol impronta su labor analítica, a saber: los Estados miembros, que pueden comunicarse con Europol por vía centralizada[32] (Unidades Nacionales de Europol) o descentralizada (los servicios nacionales designados);[33] los organismos de la Unión con los que Europol comparte su finalidad operativa,[34] como [35] la Guardia Europea de Fronteras y Costas (Frontex),[36] la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y/o la Oficina Euro-

---

30 Cdo. 26 de la Directiva (UE) 2023/977 del Parlamento Europeo y del Consejo 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 L 134 de 22.5.2023, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32023L0977 [última consulta el 20 de abril de 2024].

31 Ahora regulada por el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, DOUE L 303 de 28.11.2018, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32018R1807 [última consulta el 20 de abril de 2024], cuya relevancia se ceñirá a la regulación de datos no personales, incluidos los generados por máquinas en nuestro (también conocidos como datos sintéticos).

32 Arts. 17.1, let. a) y 7 del Reglamento Europol. Cfr., por ejemplo, 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, DOUE L 253 de 29 de septiembre de 2005, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A02005D0671-20231031 [última consulta el 20 de abril de 2024], que obliga los Estados miembros a transmitir información a Europol sobre investigación, procedimientos y condenas de delitos de terrorismo.

33 Art. 7.5 del Reglamento Europol y Tribunal de Cuentas, *Europol support to fight migrant smuggling: a valued partner, but insufficient use of data sources and result measurement*, Luxemburgo, 30 de septiembre de 2021, p. 16, disponible en: https://www.eca.europa.eu/en/publications?did=59363 [última consulta el 20 de abril de 2024].

34 Art. 88.2, let. b) del Convenio Europol.

35 Art. 17.1, let. b) del Reglamento Europol.

36 Art. 90 del Reglamento (UE) 2019/1896 del Parlamento Europeo y del Consejo, de 13 de noviembre de 2019, sobre la Guardia Europea de Fronteras y Costas y por el que se derogan los Reglamentos (UE) n.º 1052/2013 y (UE) 2016/1624, DOUE L 295 de 14.11.2019, disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32019R1896 [última consulta el 20 de abril de 2024].

pea de Lucha contra el Fraude (OLAF);[37] los países terceros y las organizaciones internacionales con los que Europol haya concluido acuerdos de cooperación; las entidades privadas[38] que reversan información en las unidades nacionales de los Estados miembros,[39] o de una parte socia afectada, mediante Europol,[40] y los particulares[41] que actúan a través de Europol para referir información al Estado miembro o tercer país de procedencia.[42]

El art. 17.2 del Reglamento Europol añade que Europol puede recuperar la información[43] por fuentes públicamente disponibles[44], o rastrearla desde las bases de datos a las que tiene acceso.[45] Se recuerda que Europol tiene acceso a los seis sistemas TI a gran escala del Espacio de Libertad, Seguridad y Justicia (ELSJ),[46] y podrá utilizar los componentes que disponen de su interoperabilidad.[47] Dentro de ellos, merecen especial atención el Sistema de Información Schengen (SIS) y el nuevo marco de Prüm II,[48] pues estos dos marcos jurídicos permiten procesar ficheros de ADN y, unirlos a la información no genética (p.e. imágenes faciales) por medio del análisis del *big data*, podrían agilizar la detección y aprensión de crímenes irresueltos, también conocidos en inglés como *cold cases*.[49] En el caso de SIS, Europol tiene derecho a consultar los ficheros conservados de forma centralizada en el C-SIS y, en determinadas circunstancias, a descárgalos.[50] Además, Europol puede intercambiar información complementaria siguiendo las instrucciones del Manual SIRENE,[51]

---

37 Eurojust y OLAF pueden acceder a los datos de Europol sobre la base de respuestas positivas o negativas a través de SIENA, pero el acceso mutuo no se ha implementado todavía.

38 Lai, Wanqi, Van Varenbergh, Amalia, y Bellaert, Wannes, «Europol and its growing Alliance with private parties», *Revue Internationale de Droit Pénal*, Vol. 92, n.º 2, 2021, pp. 45-66.

39 Que se han convertido en importantes reservas de información genómica según Shen, Hong y Ma, Jian «Privacy Challenges of Genomic Big Data» R. Cohen, Irun, Lajtha, Abel, D. Lambris, John, y Paoletti, Rodolfo (Eds) *Advances in Experimental Medicine and Biology*, Springer, Berlín, 2017, pp. 139-148.

40 Arts. 26 y 26 ter del Reglamento Europol.

41 Se exceptúan los arts. 36 y 37 del Reglamento Europol.

42 Art. 27 del Reglamento Europol.

43 Art. 17.2 del Reglamento Europol se refiere a fuentes de información públicamente disponibles, e.j. internet y datos públicos.

44 Legind Larsen, Henrik, Blanco, José María, Pastor Pastor, Raquel, y R. Yager, Ronald, *Using Open Data to Detect Organized Crime Threat: Factors Driving Future Crime*, Springer, Berlín, 2017.

45 Art. 17.3 del Reglamento Europol; en este caso, se deben respetar las normas de protección de datos personales previstas por el instrumento regulador de la base de datos accedida.

46 Vavoula, Niovi, *Immigration and Privacy in the Law of the European Union. The Case of Information Systems*, Brill/Nijhoff, Leiden, 2022.

47 Cfr. el art. 22 del Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, DOUE L 135, 22 de mayo de 2019, disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32019R0818 [última consulta el 20 de abril de 2024].

48 Reglamento del Parlamento Europeo y del Consejo 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 del Parlamento Europeo y del Consejo (Reglamento Prüm II), PE 75 2023 REV 1, Estrasburgo, 13 de marzo de 2024, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:PE_75_2023_REV_1 [última consulta el 20 de abril de 2024].

49 Europol, *Europol joins international appeal to solve murder case*, La Haya, 10 de septiembre de 2024, disponible en: https://www.europol.europa.eu/media-press/newsroom/news/europol-joins-international-appeal-to-solve-murder-case?mtm_campaign=newsletter [última consulta el 15 de septiembre de 2024].

50 Art. 48.6 del Reglamento 2018/1862.

51 Decisión de Ejecución (UE) 2016/1209 de la Comisión, de 12 de julio de 2016, por la que se sustituye el anexo de la Decisión de Ejecución 2013/115/UE de la Comisión relativa al Manual SIRENE y otras medidas de ejecución para el Sistema de Información de Schengen de segunda generación (SIS II) [notificada con el número C(2016) 4283], DOUE L 203, 28 de julio de 2016, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016D1209 [última consulta el 20 de abril de 2024].

por ejemplo, para comunicarse con el Estado miembro emisor de una alerta. Cuando recibe información complementaria, Europol la puede cotejar con sus bases de datos y Proyectos de Análisis (PA) operativos y así detectar conexiones u otros vínculos pertinentes, o llevar a cabo análisis estratégicos, temáticos u operativos.[52] Recientemente, Europol ha sido autorizado para proponer la inserción de las denominadas «alertas de información» en el SIS en el interés de la Unión, reforzando la cooperación con países terceros y organizaciones internacionales en la captura de combatientes terroristas extranjeros.[53] Es, sin embargo, el nuevo marco de Prüm II el instrumento que completa la previsión de Europol como punto neurálgico para el intercambio descentralizado de la información —en concreto, los perfiles de ADN, los datos dactiloscópicos, determinados datos de matriculación de vehículos, las imágenes faciales y los antecedentes policiales— a nivel internacional: los Estados miembros tendrán el permiso para acceder a los datos cedidos por terceras partes,[54] y Europol podrá cruzar sus datos con los ficheros nacionales,[55] junto al Registro Común de Datos (RCD) según el art. 22 del Reglamento 2019/818.[56] De esta forma, Europol puede superar las barreras regulatorias internas de cada Estado que limitan la puesta a disposición de perfiles de ADN a efectos de investigación policial.[57]

3.2. El «uso primario» de los datos de Europol y su ulterior procesamiento

La fuente por la que Europol llega a obtener la información es decisiva a la hora de determinar la primera (y ulterior)[58] finalidad perseguida en virtud de la cual Europol puede procesar la información y, sobre todo, los datos personales en el respeto del principio de la limitación de la finalidad del tratamiento.[59] El art. 19 del Reglamento Europol no define claramente qué debemos entender por primera y ulterior finalidad, como el legislador de la Unión ha hecho en otros textos jurídicos.[60] Sin embargo, esta distinción puede entenderse

---

52 Art. 2, lets. b) y c) del Reglamento Europol. Sobre el análisis cruzadp véase la Sentencia del Tribunal General, *Leon Leonard Johan Veen c Agencia de la Unión Europea para la Cooperación Policial (Europol)*, 27 de abril de 2022, ECLI:EU:T:2022:261.

53 Art. 4.1, let. t) del Reglamento Europol y Vavoula, Niovi «Surveillance of Foreign Terrorism Fighters via the Schengen Information System (SIS): Towards Maximum Operationalisation of Alerts and an Enhanced Role for Europol», *New Journal of European Criminal Law*, 2023, Vol. 2, n.º 14, pp. 206-230.

54 Cdo. 20 del Reglamento Prüm II.

55 Cdo. 25 del Reglamento Prüm II y, en el caso de España, cfr. la Secretaria de Estado de Seguridad, *Base de datos policial de identificadores obtenidos a partir de ADN*, Madrid, enero-diciembre 2022, disponible en: https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/Base-de-datos-policial-de-identificadores-obtenidos-a-partir-de-ADN.-Memoria/Base_de_datos_policial_identificadores_ADN_Memoria_2022_126200173_web.pdf [última consulta el 20 de abril de 2024].

56 Tassinari, Francesca *Data Protection and Interoperability in EU External Relations: Guaranteeing global data transfers in the area of freedom, security and justice*, Brill/Nijhoff, Leiden, en prensa.

57 Westermark, Henrik, Aronovitz, Alberto, Curran, John, Fausch, Inesa, Fournier, Johanna, Hohenecker, Lukas, Kleczewski, Anne-Grace Pretelli, Ilaria, Polanco Lazo, Rodrigo, Topaz Druckman, Karen, Viennet, Carole, Went, Floriaan, Zheng, Jun *The Regulation of the Use of DNA in Law Enforcement*, Instituto suizo de derecho comparado, Lausanne, 2020.

58 Se entiende por "uso ulterior" el tratamiento de los datos personales «para otro fin distinto de aquel para el que se recogieron los datos personales» según indica el art. 6.4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679 [última consulta el 20 de abril de 2024].

59 A falta de un listado de principios en el propio Reglamento Europol, nos remitimos al art. 71.1, let. b) del RPDUE tal y como explicamos en Tassinari, Francesca, «Issues of consistency and complementarity in EU privacy law: The Europol's Big Data challenge», *Revista General de Derecho Europeo*, n.º 63, pp. 133-169.

60 Distinción, la del primer y segundo uso, que encontramos (por ejemplo) en el nuevo Reglamento sobre el Espacio Europeo de Datos Sanitarios cuya publicación en el DOUE esperamos que ocurra prontamente. Ya sobre la propuesta de re-

del art. 19.1, párrafo 3.º, del Reglamento Europol que establece: «Europol tratará la información con fin distinto a aquel para el que fue facilitada solo si así lo autoriza el proveedor de la información». Entendemos por «primera finalidad» o «primeras finalidades» aquella(s) comunicada(s) por el Estado miembro, organismo de la Unión, tercer país u organización internacional en el momento de facilitar la información a Europol de conformidad con el art. 18 del Reglamento Europol.[61] Si la parte transmitente no cumple con este requisito, o Europol recauda él mismo la información, o la información ha sido cedida por entidades privadas o particulares, compete a Europol establecer la pertenencia y finalidad(es) del primer tratamiento.[62] Cualquier uso posterior, y diferente, es «ulterior» respecto a la(s) primera(s) indicada(s), siendo inapropiado, en nuestro juicio, utilizar las expresiones de «uso secundario, terciario, cuarto» y así discurriendo puesto que «[…] es impropio de la jerga de la protección de datos personales ya que alude, de un modo un tanto genérico, a todos aquellos usos que sean significativamente distintos respecto del contexto, origen o finalidad primigenias de los datos».[63] En cualquier caso, la primera(s) finalidad(es) perseguida(s) debe(n) atenerse tanto a los propósitos perseguibles por Europol en virtud del art. 18 del Reglamento Europol[64] (y sus Anexos I y II), como a los límites legales previstos por la base jurídica eventualmente afectada.[65] Por ejemplo, en el caso del SIS, las alertas a las que Europol accede podrán ser (re)procesadas, eventualmente, siempre y cuando el fin ulterior perseguido guarde «[…] relación con algún caso concreto y [esté] justificado por la necesidad de prevenir una amenaza grave e inminente para el orden y la seguridad públicos, por razones graves de seguridad nacional o por la necesidad de prevenir un delito grave. A tal fin, deberá obtenerse autorización previa del Estado miembro emisor».[66] De hecho, el Reglamento 2018/1862 considera en su art. 56.6 que todo uso ulterior de los datos del SIS que no cumpla con esta norma debe considerarse como una «desviación de la finalidad con arreglo al Derecho nacional de cada Estado miembro y estará sujet[o] a sanciones de conformidad con el artículo 73».

Ahora bien, entendemos que el uso ulterior de los datos personales puede darse, bien porque Europol decide procesar la información para una finalidad distinta a la inicialmente perseguida, bien porque los datos son puestos a disposición de actores que pretenden reutilizarlos para un fin diferente. En ambos casos, Europol deberá atenerse a las restricciones de acceso o uso impuestas por el proveedor de la información,[67] cuando estas resulten aplicables.[68] Es, por lo tanto, crucial que el propio proveedor de la información (o Eu-

---

glamento véase DE MIGUEL BERIAIN, Iñigo «El uso de datos de salud para investigación biomédica a la luz de la Propuesta de Reglamento del Parlamento Europeo del Consejo sobre el Espacio Europeo de Datos Sanitarios», *Revista jurídica de Castilla y León,* n.º 60, 2023, pp. 7-35.

61 Art. 18.1 del Reglamento Europol.

62 Art. 18.1, párrafo 2º, del Reglamento Europol.

63 En la misma línea, pero en otro contexto, RECUERO LINARES, Mikel «El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales» *InDret*, n.º 2, 2024, pp. 525-551, p. 534.

64 Art. 18.2, lets. de a) a f) del Reglamento Europol se refieren a: los controles cruzados destinados a identificar conexiones u otras relaciones pertinentes entre datos relacionados con las personas indicadas en las lets. i) y ii); análisis estratégicos o temáticos; análisis operativos; intercambios más agiles de información entre Estados miembros, Europol, otros organismos de la Unión, terceros países, organizaciones internacionales y entidades privadas; proyectos de investigación e innovación, y actividades destinadas a apoyar a los Estados miembros, previa solicitud de estos, a la hora de informar al público sobre los sospechosos o las personas condenadas en búsqueda sobre la base de una resolución judicial nacional relativa a un delito que se incluya en los objetivos de Europol, y a facilitar que el público proporcione información sobre dichas personas a los Estados miembros y a Europol.

65 Art. 17(3) del Reglamento Europol, en la medida en que prevean normas de acceso y utilización más estrictas que las establecidas por el Reglamento Europol.

66 Art. 56.5 del Reglamento 2018/1862.

67 GOIZUETA VÉRTIZ, Juana «La cooperación policial en el seno de Europol: el principio de disponibilidad y la confidencialidad de la información», *Revista Española de Derecho Constitucional*, n.º 110, pp. 75-103.

68 No es el caso de los datos personales que Europol recaude por sí solo, ya que el art. 19.3 del Reglamento Europol afirma que: «[…] Europol podrá imponer restricciones de acceso o utilización por parte de los Estados miembros, or-

ropol cuando le competa en los casos señalados) realice el test sobre la compatibilidad de la finalidad(es) primariamente perseguida(s)[69] y el uso ulterior según el derecho aplicable. En el caso de que el proveedor sea un Estado miembro, el art. 9 de la Directiva 2016/680[70] (DPDP) sobre «condiciones de tratamiento específicas» establece que el uso de los datos personales recogidos por las autoridades competentes en virtud del art. 1 de la DPDP para una finalidad distinta que las establecidas en el mismo artículo debe estar autorizado por el Derecho de la Unión o del Estado miembro, de conformidad con el RGPD «a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión». Es decir, debemos siempre contar con una base jurídica en derecho que autorice el uso ulterior de los datos personales cuando estos habían sido recogidos inicialmente por las autoridades competentes de la DPDP. Sin embargo, el uso ulterior se regularía por el RGPD siempre y cuando esté amparado por la aplicación del derecho de la Unión; si no, la DPDP no impone ninguna limitación, pudiéndose el procesamiento de datos personales regularse por el derecho nacional o quedar totalmente descubierto cuando el derecho de la UE no es aplicable.

Respecto al primer punto (el uso de la información por Europol para una finalidad ulterior distinta a la inicialmente perseguida) del Reglamento Europol desprendemos que el personal de Europol está legalmente legitimado a reusar la información para fines de investigación científica e innovación cuando los datos habían sido recogidos inicialmente para fines de verificación cruzada, análisis estratégico, análisis de riesgo o temático y de facilitación del intercambio de información entre Estados miembros, Europol, otros órganos de la Unión, países terceros, organizaciones internacionales y partes privadas.[71] Esta disposición complementa el art. 9.1 de la DPDP, siendo Derecho de la Unión que autoriza el ulterior tratamiento, lo que nos exige respetar el RGPD y, en concreto, su art. 6.4. De cara al segundo punto (el uso de la información de Europol por otros actores para una finalidad ulterior distinta a la inicialmente perseguida) la situación es más compleja, pues el régimen varía dependiendo del actor implicado.

Los Estados miembros pueden acceder de forma directa a la información facilitada para verificación cruzada y análisis estratégicos o temáticos según se desprenda de la legislación nacional;[72] en el caso de análisis operativos el acceso es indirecto (*hit/no-hit*)[73] y, excepcionalmente, directo según el PA operativo en cuestión.[74] Una vez accedidos, y salvo restricciones, los datos de Europol pueden ser rehusados para fines de prevención, detección, investigación y enjuiciamiento de las formas de delincuencia para las que Europol es competente, y otras formas de delincuencia grave según se recoge en la orden de detención y entrega europea.[75] El régimen del uso ulterior de los datos personales es por ende más restrictivo respecto al

---

ganismos de la Unión, países terceros y organizaciones internacionales de la información extraída de fuentes públicas».

69 Art. 6.4 del RGPD.

70 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DOUE L 119 de 4.5.2016 (DPDP en adelante), disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016L0680 [última consulta el 20 de abril de 2024].

71 Art. 19 del Reglamento Europol y véase *infra* el análisis sobre las tareas del art. 18.2 del Reglamento Europol.

72 Art. 20 del Reglamento Europol.

73 Art. 20.2 del Reglamento Europol.

74 Art. 20.2 bis del Reglamento Europol.

75 Art. 20.3 del Reglamento Europol y Decisión Marco 2002/584/JAI del Consejo, e 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros - Declaraciones realizadas por algunos Estados miembros con ocasión de la adopción de la Decisión marco, DOUE L 190 de 18.7.2002, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32002F0584 [última consulta el 20 de abril de 2024].

contemplado por la DPDP. Por lo contrario, nada se establece respecto al uso ulterior de los datos por parte de la Fiscalía Europa, Eurojust, y OLAF, que solo acceden a los datos de Europol de forma indirecta (*hit/no-hit*),[76] razón por la que resulta imprescindible remitirnos a los convenios de colaboración subyacentes para determinar la posibilidad del uso ulterior de los datos de Europol. El art. 10.1 del acuerdo de trabajo entre la Fiscalía Europea y Europol de 2021,[77] el art. 13.2 del acuerdo entre Eurojust y Europol del 2010,[78] y el art. 11.1 del acuerdo de trabajo entre OLAF y Europol de 2020[79] prevén que, en un principio, la información (incluidos los datos personales) transmitida de una parte a la otra solo puede ser usada para la finalidad por la que fue cedida. Sin embargo, los acuerdos de trabajo concluidos con la Fiscalía Europea y OLAF permiten, en sus arts. 13.2 y 10.2 respectivamente, el uso ulterior de la información: el primero, cuando la parte transmitente lo autoriza y, el segundo, cuando el uso ulterior es compatible con el primero. Finalmente, la comunicación de datos personales a terceras partes se regula (aun en gran medida) por los acuerdos de cooperación celebrados antes del 1 de mayo de 2017.[80] Estos acuerdos exigen la autorización previa de los Estados miembros que hayan transmitido la información,[81] y (generalmente)[82] limitan el uso de los datos personales para la finalidad por la que los datos han sido comunicados, salvo que la parte transferente autorice el uso ulterior de forma expresa.[83] En esta línea, los acuerdos de cooperación con Canadá,[84] Dinamarca,[85] Georgia,[86] la República de Moldova,[87] la República de Serbia,[88] el Principado de Liechtenstein,[89] Ucrania,[90] Albania,[91] Bosnia y Herzegovina,[92] Montenegro,[93] los EE.UU,[94] y el Reino Unido[95] permiten el uso ulterior de la información si la parte remitente lo autoriza. Además, el acuerdo entre Europol y el Reino de Noruega permite el uso ulterior de los datos personales en el caso de que estos hayan sido requeridos en el marco de una investigación específica a cargo de Europol.[96] De forma más articulada, los acuerdos de cooperación concluidos con Australia, Noruega, Colombia, Islandia, la Republica de Macedonia del Norte, Suiza y Mónaco prevén que, si los datos personales son transmitidos espontáneamente, la parte

---

76 Arts. 20 bis y 21 del Reglamento Europol.

77 Acuerdo de trabajo entre la Fiscalía Europea y Europol, disponible en: https://www.eppo.europa.eu/sites/default/files/2021-01/EPPO%20_Europol_Working_Arrangement.pdf [última consulta el 20 de abril de 2024].

78 Acuerdo entre Eurojust y Europol del 1 de enero de 2010, disponible en: https://www.eurojust.europa.eu/sites/default/files/InternationalAgreements/Eurojust-Europol-2010-01-01-EN.pdf [última consulta el 20 de abril de 2024].

79 Acuerdo de trabajo entre OLAF y Europol, disponible en: https://anti-fraud.ec.europa.eu/document/download/39a5bd85-23da-4dfe-8c10-5fe67f73b505_fr?filename=working_arrangements_olaf_europol_en.pdf [última consulta el 20 de abril de 2024].

80 Art. 25.1, let. c) del Reglamento Europol y Rosanó, Alessandro «Protecting Europe beyond its Borders: The Agreements between Europol and Third States or International Organizations», *Cadernos de Dereito Actual*, n.º 4, 2016, pp. 9-21.

81 Art. 23.6 del Reglamento Europol.

82 Se exceptúan el acuerdo de cooperación entre Europol y Nueva Zelanda que no impone ninguna limitación *a priori*.

83 Los acuerdos de cooperación concluidos por Europol están disponibles en el siguiente enlace: https://www.europol.europa.eu/partners-collaboration/agreements [última consulta el 20 de abril de 2024].

84 Art. 6.5 del acuerdo de cooperación entre Europol y Canadá.

85 Art. 12.2 del acuerdo de cooperación entre Europol y Dinamarca.

86 Art. 12.2 del acuerdo de cooperación entre Europol y Georgia.

87 Art. 12.2 del acuerdo de cooperación entre Europol y la República de Moldova.

88 Art. 12.2 del acuerdo de cooperación entre Europol y la República de Serbia.

89 Art. 12.2 del acuerdo de cooperación entre Europol y el Principado de Liechtenstein.

90 Art. 12.2 del acuerdo de cooperación entre Europol y el Ucrania.

91 Art. 12.2 del acuerdo de cooperación entre Europol y Albania.

92 Art. 12.2 del acuerdo de cooperación entre Europol y Bosnia Herzegovina.

93 Art. 12.2 del acuerdo de cooperación entre Europol y Montenegro.

94 Art. 5.3 del acuerdo de cooperación entre Europol y los EE.UU.

95 Art. 7.2 del acuerdo entre Europol y el Reino Unido.

96 Art. 9.2, let. i) del acuerdo de cooperación entre Europol y el Reino de Noruega.

remitente debe indicar las restricciones aplicables al uso de los datos, cancelación o destrucción de estos en el momento de su transmisión. Esta expresión, a nuestro entender, podría abrir una brecha para el uso ulterior de los datos personales transmitidos en el caso de que Europol así lo indicara. La tabla de abajo pone de relieve la finalidad por la que Europol puede procesar la información sobre la base del art. 18.2 del Reglamento Europol, las categorías de datos personales procesables en virtud del Anexo II, y el posible uso ulterior de los datos para una finalidad distinta que la primigenia.

Tabla I

Uso primario y uso ulterior de los datos personales según el mandato de Europol

Ámbito	Finalidad	Datos	Uso ulterior	Acceso
Delitos del Anexo I y delitos conexos	Verificación cruzada	Datos procesados según el Anexo II	— Por autorización del proveedor de la información; — Para proyectos de investigación e innovación.	— Funcionarios de Europol; — Funcionarios de enlace de los Estados miembros; — Expertos Nacionales en Comisión de Servicio en Europol; — Unidades Nacionales de Europol; — Socios de Europol por su centro operativo; — Eurojust y OLAF, salvo restricciones del proveedor.
	Análisis estratégico, operativo, y apoyo en intercambio de información con Estados miembros, organismos de la Unión, países terceros y organizaciones internacionales	Datos procesados según el Anexo II	— Por autorización del proveedor de la información; — Para proyectos de investigación e innovación; — Datos personales tratados a efecto de un PA operativo para otro PA.	— Funcionarios de Europol; — Funcionarios de enlace de los Estados miembros; — Expertos Nacionales en Comisión de Servicio en Europol; — Unidades Nacionales de Europol; — Socios de Europol por su centro operativo; — Eurojust y OLAF, salvo restricciones del proveedor. * En el caso de PA para el análisis operativo, los usuarios se definen en el propio PA.
	Proyectos de investigación e innovación	Categorías de interesados no comprendidas en el Anexo II		— Funcionarios de Europol; — Funcionarios de enlace de los Estados miembros; — Expertos Nacionales en Comisión de Servicio en Europol; — Unidades Nacionales de Europol; — Socios de Europol por su centro operativo; — Eurojust y OLAF, salvo restricciones del proveedor.

Ámbito	Finalidad	Datos	Uso ulterior	Acceso
Delitos del Anexo I y delitos conexos	Apoyo de una investigación penal (análisis operativo y verificación cruzada)	Categorías de interesados no comprendidas en el Anexo II	— Por autorización del proveedor de la información; — Para proyectos de investigación e innovación.	— Funcionarios de Europol; — Funcionarios de enlace de los Estados miembros; — Expertos Nacionales en Comisión de Servicio en Europol; — Unidades Nacionales de Europol; — Socios de Europol por su centro operativo; — Eurojust y OLAF, salvo restricciones del proveedor.
	Determinación de su relevancia respecto al art. 18.5 del Reglamento Europol	Categorías de interesados no comprendidas en el Anexo II	— Cualquier uso(s) establecido(s) por el art. 18.5 del Reglamento Europol	— Funcionarios de Europol, salvo restricciones del proveedor.

Fuente: elaboración propia.

3.3. La delimitación funcional del mandato de Europol y el desafío del *big data*

Como hemos mencionado más arriba, la información que Europol puede procesar está delimitada funcionalmente por el ámbito competencial de su mandato en virtud del art. 18 del Reglamento Europol, junto a los Anexos I y II. El Anexo I enumera las formas graves de delitos por las que Europol puede prestar apoyo a dos o más Estados miembros, incluido el terrorismo, y que pueden llegar a afectar un interés común protegido por la Unión; el art. 3.2 extiende la competencia de Europol a los delitos «conexos» a los objetivos perseguidos por la Agencia.[97] El Anexo II lista las categorías de interesados cuyos datos pueden ser procesados por Europol y las correspondientes categorías de datos personales según la finalidad perseguida: la verificación cruzada;[98] el análisis estratégico u operativo; y el apoyo para el intercambio de información con Estados miembros, organismos de la Unión, países terceros y organizaciones internacionales.[99] Siguiendo al SEPD,[100] el Anexo II era el punto de referencia que servía para controlar no solo que Europol no actuase *ul-*

[97] En concreto: los delitos cometidos con objeto de procurarse los medios para perpetrar actos en los que Europol sea competente; los delitos cometidos para facilitar o perpetrar actos en los que Europol sea competente; y los delitos cometidos para asegurar la impunidad de quienes cometan estos actos en los que Europol sea competente.

[98] Anexo II, let. A punto 1, lets. a) y b) se remiten a: personas sospechosas de haber cometido o participado en un delito de competencia de Europol, o que haya sido condenada por tal delito; y personas de las que existan indicios concretos o motivos razonables para pensar que cometerá delitos de competencia de Europol.

[99] Anexo II, let. B punto 2, lets. c) y v) lista a: personas sospechosas de haber cometido o de haber participado en un delito que es competencia de Europol o que hayan sido condenadas por tal delito; personas respecto de las cuales existan indicios concretos o motivos razonables, de acuerdo con el Derecho nacional del Estado miembro de que se trate, para pensar que cometerán delitos que son competencia de Europol; personas que podrían ser citadas como testigos en investigaciones sobre los delitos en cuestión o en futuras causas penales; personas que hayan sido víctimas de uno de los delitos en cuestión o respecto de las cuales existan motivos para pensar que podrían ser víctimas de tales delitos; personas de contacto y asociados, y personas que puedan facilitar información sobre los delitos en cuestión.

[100] SEPD, *Decision on the retention by Europol of datasets lacking Data Subject Categorisation,* Bruselas, 21 de diciembre de 2021, p. 2.

tra vires respecto al Reglamento 2016/794,[101] sino que también tratase la información en modo adecuado, pertinente y limitado en relación con los fines perseguidos en el respeto del principio de la minimización de datos.[102] Sin embargo, la previsión de unos catálogos exhaustivos de delitos y categorías de interesados afectados, que delimitasen de forma minuciosa el ámbito de actuación de esta Agencia, fue cuestionada en el episodio conocido como el *Europol's Big Data challenge*.

En el año 2020,[103] el SEPD alertó de que los Estados miembros habían estado transmitiendo conjuntos de datos voluminosos y complejos a Europol —es decir, conjuntos de datos que, debido a su volumen, naturaleza o formato de los datos no podían procesarse en la red operativa de Europol— solicitando su análisis para detectar vínculos con otros delitos de alcance transnacional.[104] Así Hoek y Stigter[105] recuerdan que Europol recibió de Francia 16.7 terabytes de datos después de los atentados de París y, a raíz de esta petición, el grupo de trabajo *Fraternité* examinó los datos remitidos con el programa Palantir Gotham.[106] El problema principal se ceñía al hecho de que estos datos no podían someterse a un proceso previo de categorización y extracción[107] de tal manera que la información remitida habría podido desbordar los límites previstos por el Anexo II del Reglamento Europol. Europol, por su parte, habría debido tratar los datos recibidos durante el tiempo necesario para apoyar cada investigación penal específica, incumpliendo con el principio de la limitación del plazo de conservación.[108]

A raíz de la investigación impulsada por el SEPD, Europol fue advertido de incurrir en la infracción de los arts. 18.3, 18.5, 28.1, let. c) y Anexo II.B del Reglamento 2016/794. Según el SEPD[109] las restricciones a los principios de minimización de datos, limitación de la conservación, y limitación de la finalidad perseguida eran desproporcionadas e infringían indebidamente los derechos fundamentales a la vida privada y a la protección de los datos personales de las personas afectadas.[110] Antes de todo, y si bien la retención de datos personales en el interés de la investigación, detección y enjuiciamiento de delitos graves[111] podría provocar injerencias graves en los derechos de las personas,[112] las limitaciones impuestas no podían sobrepasar los límites de lo «estrictamente necesario».[113] A este efecto, el Tribunal de Justicia de la UE (TJUE) invalidó la Directiva sobre retención de datos de tráfico por afectar «prácticamente a toda la población europea […] sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que

---

101 Versión consolidada del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (Reglamento Europol en adelante, salvo especificar otra cosa) DOUE L 135 de 24.5.2016, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A02016R0794-20220628 [última consulta el 20 de abril de 2024].

102 El principio de la minimización de datos se recoge en el art. 71.1, let. c) del RPDUE.

103 SEPD, *Decision on the own initiative inquiry on Europol's big data challenge*, Bruselas, 18 de diciembre de 2020.

104 Cdo. 22 del Reglamento 2022/991.

105 Hoek, Dante y Stigter, Jill «Europol: an overwhelming stream of Big Data», *Revue Internationale De Droit Pénal*, Vol. 2, n.º 92, 2021, pp. 19-44, p. 24.

106 Este fue implantado por la consultora Capgemini, según las preguntas escritas que los eurodiputados Cornelia Ernst (GUE/NGL), Patrick Breyer (Verts/ALE) y Mathilde Androuët (ID) enviaron a la Comisión europea el 1 de julio de 2020, el 10 de marzo de 2022 y el 19 de enero de 2024, respectivamente.

107 En cada PA, Europol debe establecer las categorías de interesados, el ámbito delictivo, la pertinencia operativa de acuerdo con el proveedor de los datos.

108 Satpathy, Suneeta y Mohanty, Sachi *Big Data Analytics and Computing for Digital Forensic Investigations*, CRC Press, BocaRaton/Oxon, 2020.

109 SEPD, *Opinion 4/2021 on the Proposal for Amendment of the Europol Regulation*, Bruselas, 8 de marzo de 2021, p. 11.

110 Arts. 7, 8 y 52.1 de la CDFUE.

111 Sentencia del Tribunal de Justicia (Gran Sala), *Digital Rights Ireland Ltd,* de 8 de abril de 2014, ECLI:EU:C:2014:238, párrafo 49.

112 Sentencia del Tribunal de Justicia (Gran Sala), *Privacy International*, 6 de octubre de 2020, ECLI:EU:C:2020:790.

113 *Digital Rights Ireland Ltd* párrafo 52.

pueda dar lugar a acciones penales».[114] En la jurisprudencia del TJUE se prohíbe, por lo tanto, el acceso descontrolado a los datos de personas que no están relacionadas con los delitos graves, de forma directa o indirecta, por parte de las autoridades de policía. El TJUE exige delimitar temporalmente y geográficamente el «circulo de personas que pueden estar implicadas de una manera u otra en un delito grave».[115] Además, el periodo de conservación de los datos debe poder fijarse en función de las categorías de datos procesadas, según criterios objetivos,[116] y se prohíbe la conservación generalizada e indiferenciada de manera sistemática y continuada a favor de las investigaciones policiales.[117] Es más, tanto el acceso a los datos, como el uso posterior, deberían limitarse a un número estricto de personas para los «fines de prevención y detección de delitos graves delimitados de forma precisa o al enjuiciamiento de tales delitos».[118] La falta de estos parámetros impide calcular el grado de injerencia provocado en los derechos de las personas y no puede justificarse en una sociedad democrática.[119]

Europol fue entonces llamada a suprimir los datos personales de las personas no vinculadas a una investigación policial, y a redirigir el procesamiento de conjuntos de datos voluminosos y complejos dentro de los límites de la Carta de Derechos Fundamentales de la UE (CDFUE).[120] El 17 de noviembre de 2020 Europol presentó un plan de acción[121] que acordase la modificación del Reglamento 2016/794 sobre la base de cinco pilares: 1. el marcado de conjuntos de datos sin categorización de interesado (DSC en inglés) por el proveedor; 2. el etiquetado de datos sin DSC en el entorno de Europol; 3. el acceso restringido a los mismos; 4. unas revisiones trimestrales; y 5. el nombramiento de un coordinador de control para la calidad de los datos. En diciembre 2021, el SEPD reclamó[122] la falta de un período máximo de conservación de los datos sin DSC y propuso un plazo máximo de seis meses de conformidad con el art. 18.6 del Reglamento 2016/794, más un período transitorio de doce meses para los conjuntos de datos "flotantes" en el entorno de Europol. Sin embargo, Europol no se conformó y contestó que el art. 18.6 del Reglamento 2016/794 servía para averiguar si procesar la información de cara a las tareas del art. 18.2 de su mandato, pero no para comprobar si la información entraría en las categorías y extracciones pertinentes para los PA operativos. Europol revindicó un periodo de doce meses más seis, exceptuando los casos específicos de investigación criminal ya en curso (e.j., Equipos Conjuntos de Investigación o grupos operativos). Además, Europol reclamaba que los datos deberían conservarse tanto tiempo como fuese necesario y proporcionado para apoyar la investigación en cuestión, y preservar la cadena de pruebas.[123]

El reto del *big data* de Europol sirvió de detonante para modificar el Reglamento 2016/794 por el Reglamento 2022/991[124] y permitir el procesamiento de categorías de personas no mencionadas en el Anexo II.

---

114 *Ibid*. párrafos 57-58.

115 *Ibid*. párrafo 59.

116 *Ibid*. párrafo 63.

117 Sentencia del Tribunal de Justicia (Gran Sala), *Tele2 Sverige AB*, 21 de diciembre de 2016, ECLI:EU:C:2016:970, párrafo 97.

118 *Digital Rights Ireland Ltd* párrafo 61 y *Tele2 Sverige AB* párrafo 114.

119 *Tele2 Sverige AB* párrafo 106.

120 Carta de los Derechos Fundamentales de la Unión Europea, DOUE C 202 de 7.6.2016, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12016P%2FTXT [última consulta el 3 de mayo de 2024].

121 EUROPOL, *Action Plan of 17 November 2020 addressing the risks raised in the EDPS Decision on 'Europol's Big Data Challenge*, La Haya, 17 de noviembre de 2020.

122 SEPD, *Decision on the retention by Europol of datasets lacking Data Subject Categorisation*, Brusuelas, 21 de diciembre de 2021.

123 Como señala NICOLÁS JIMÉNEZ *cit.* nota n.º 21, p. 88: «[…] se debe apreciar la diferencia entre el almacenamiento de perfiles de ADN con fines de investigación policial, práctica para la que, como ya dijimos es necesaria una regulación específica; y su recogida para una investigación concreta, diligencia también necesitada de un desarrollo legislativo pero por motivos procesales».

124 TAS, Sarah «The dangerous increasing support of Europol in national criminal investigations: An additional layer of complexity», *New Journal of European Criminal Law*, 2023, Vol. 0, n.º 0, pp. 1-18.

El art. 18 bis del Reglamento Europol autoriza a un Estado miembro, la Fiscalía Europea, o Eurojust a facilitar datos de investigación a Europol para fines de análisis operativo o, excepcionalmente, de verificación cruzada.[125] Europol, por su parte, debe determinar el ámbito de la investigación criminal en curso mediante la agrupación de los identificadores remitidos por el proveedor de la información, lo que debe documentar en una orden de apoyo que incluye: la descripción de las investigaciones suportadas; el tipo de soporte pedido a Europol; los nombres de los países y órganos de la Unión implicados; la confirmación del proveedor de que la investigación está en curso, y los identificadores nacionales o de Europol relevantes.[126] Antes de proceder, Europol debe valorar la imposibilidad de cumplir con la petición recibida sin sobrepasar los límites previstos por el Anexo II del Reglamento Europol.[127] En virtud del art. 18 bis, Europol puede tratar los datos de investigación de conformidad con el art. 18.2 durante todo el tiempo de apoyo de la investigación penal específica en curso,[128] e incluso después de este periodo, a petición del proveedor u otro Estado miembro en el que esté tramitándose un procedimiento judicial relacionado con una investigación penal conexa, «con el fin de garantizar la veracidad, fiabilidad y trazabilidad del proceso de inteligencia criminal, y únicamente durante el tiempo en que se esté tramitando el procedimiento judicial relacionado con la investigación penal específica para la que se hayan facilitado dichos datos».[129] Los datos de investigación así remitidos a Europol deben estar funcionalmente separados de otros datos y se pueden tratar solo si es necesario y proporcionado.[130] De forma similar, Europol puede recibir datos de investigación de un tercer país para apoyar a la investigación de uno o más Estados miembros,[131] en cuyo caso, le competería averiguar la proporcionalidad de los datos recibidos y el respeto de los derechos humanos (aunque no se sabe bien de qué forma).

Como complemento del art. 18 bis, el art. 18 ha sido dotado de un ulterior párrafo 6 bis que permite a Europol procesar información, no para averiguar su relevancia respecto a las tareas del art. 18.2, sino para comprobar si su procesamiento cumple con el art. 18.5 del Reglamento Europol, eso es, si la información entra dentro de las categorías del Anexo II y de las extracciones relevantes para sus PA. A tal efecto, Europol puede comparar estos datos con todos los demás almacenados en su nueva infraestructura informática. En definitiva, bajo su nuevo mandato, Europol ha sido autorizado para procesar categorías de interesados que quizás no estén incluidas dentro del ámbito de su competencia, autorización que podría cuestionarse al amparo de la jurisprudencia del TJUE citada más arriba. El art. 18.6 bis permite a Europol pre-analizar la información durante un período máximo de dieciocho meses a partir del momento en que Europol comprueba que dichos datos entran dentro del art. 18.5. Sin embargo, este periodo podría alargarse en casos justificados en función de la sensibilidad de la investigación, la importancia de los datos en cuestión, la naturaleza de los datos,[132] y siempre que Europol informe al SEPD dentro del plazo de un mes desde que se haya adoptado la prórroga. En cualquier caso, el período máximo de tratamiento tiene un tope de tres años.[133]

---

[125] Art. 18 bis.2 del Reglamento Europol.

[126] Consejo de Administración, *Management Board Decision on the conditions related to the processing of personal data on the basis of Article 18a of the Europol Regulation*, La Haya, 26 de junio de 2023,

[127] Art. 18 bis.1, let. b) del Reglamento Europol.

[128] Art. 18 bis.3 del Reglamento Europol.

[129] Art. 18 bis.4 del Reglamento Europol.

[130] Art. 18 bis.5 del Reglamento Europol.

[131] Art. 18 bis.6 del Reglamento Europol.

[132] Sánchez Rubio, Ana «Reflexiones sobre la todavía polémica prueba de ADN: análisis de tres posibles escenarios de su inadmisión probatoria», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º 52, 2020, pp. 169-193.

[133] Cfr. Consejo de administración, *Decision on the conditions related to the processing of data on the basis of Article 18(6a) of the Europol Regulation*, La Haya, 21 de marzo de 2023.

Tal y como ha sido presentado, el art. 18 bis fue criticado[134] por pasar por lo alto algunas de las advertencias realizadas por el SEPD —i.e., el término de seis meses para realizar el pre-análisis— sobre la base de la CDFUE. El SEPD decidió recurrir ante el Tribunal General (TG) los arts. 74 bis y 74 ter del Reglamento 2022/991,[135] pues estas normas extenderían el ámbito de aplicación de los arts. 18.5 y 18 bis a los datos recibidos por Europol antes del 28 de junio de 2022. La aplicación retroactiva del Reglamento 2022/991 menoscabaría la independencia y las competencias del SEPD por anular la resolución del 3 de enero de 2022 en vía de hecho. Sin embargo, el TG inadmitió el recurso por apreciar la falta de *ius standi* del SEPD y su no afectación directa en virtud del art. 263 del TFUE.[136] Por tanto, la cuestión sobre la validez de los arts. 18.5 y 18 bis del Reglamento Europol permanece, a día de hoy, sin respuesta.

4. El tratamiento de los datos genéticos por parte de Europol

4.1. Hacia la previsión de una regulación reforzada para el procesamiento de los perfiles de ADN en el mandato de Europol

Si bien el Convenio Europol no lo explicitaba,[137] Europol desde siempre[138] ha procesado perfiles de ADN[139] de las personas que se sospechaba hubiesen cometido un delito, o de las que se presumía que lo hubieran cometido.[140] También podía procesar los perfiles de las personas intermediarias y acompañantes, así como los de las víctimas, posibles testigos y demás informadores eventualmente.[141] A raíz de las referencias al Convenio 108[142] y a la Recomendación R(87) 15 de 17 de septiembre de 1987[143] hecha por el Convenio Europol,[144] el Acta del Consejo de 3 de noviembre de 1998 detalló las normas de protección de da-

---

134 Quintel, Teresa «The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation: The Question of Legitimizing Unlawful Practices», *European Data Protection Law Review*, Vol. 1, n.º 8, 2022, pp. 90-102.

135 Sentencia del Tribunal General, *SEPD c Parlamento y Consejo*, 6 de septiembre de 2023, ECLI:EU:T:2023:522.

136 Liñán Nogueras, Diego Javier «El sistema jurisdiccional de la Unión Europea» Mangas Martín, Araceli y Liñán Nogueras, Diego Javier (Eds) *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, pp. 473-506, p. 481.

137 Art. 8.2, punto 5), incluye dentro de la información procesada por el SIE datos que revelan «otras características útiles para su identificación, en particular rasgos físicos específicos, objetivos y permanentes». Además, el art. 10.2, se remitía al art. 6 del Convenio 108 que, aun no mencionando los datos genéticos, se refería a los datos relativos a la salud de la persona.

138 Johnson, Paul y Williams, Robin «Internationalizing New Technologies of Crime Control: Forensic DNA Databasing and Datasharing in the European Union», *Policing & Society*, Vol. 2, n.º 17, 2007, pp. 103-118, p. 108.

139 Nicolás Jiménez, Pilar «Ficheros policiales de perfiles ADN (Comentario al art. 22 LOPD)» Troncoso Reigada, Antonio (Ed) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Thomson Reuters Aranzadi, Pamplona, 2010, pp. 1428-1456, p. 1430.

140 En 2022, la base de datos SOC - iBase (Crímenes Graves y Organizados) y la base de datos CT - Palantir (Antiterrorismo) almacenaba 479 perfiles de ADN de los que 303 identificados y 179 no identificados. De estos, 115 y 63 perfiles de ADN de identificados y no identificados respectivamente habían sido retenidos por un periodo superior a los cinco años. Cfr. Europol, *Annual reporting to EDPS on Art. 30 and 31 of ER*, EDOC 1266849, La Haya, 8 de noviembre de 2022 [documento divulgado el 7 de junio de 2024].

141 Art. 6 del Acto del Consejo de 3 de noviembre de 1998 por el que se aprueban las normas aplicables a los ficheros de análisis de Europol, DOUE C 26 de 30.1.1999, disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1713974389034&uri=CELEX%3A31999F0130%2802%29, [última consulta el 20 de abril de 2024].

142 Consejo de Europa, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, 28 de enero de 1981, ETS No 108, ratificado por España con *BOE* n.º 274, de 15 de noviembre de 1985, disponible en https://www.boe.es/buscar/doc.php?id=*BOE*-A-1985-23447, [última consulta el 20 de abril de 2024].

143 Consejo de Europa, Recomendación n.º R (87) 15 que regula del uso de datos personales en el sector policial, 17 de septiembre de 1987.

144 Art. 10.1 del Convenio Europol.

tos personales aplicables a todas las categorías de datos, incluidos los FTA (Ficheros de Trabajo de Análisis) de Europol.[145] Sin embargo, ninguna de estas normas preveía una protección específica y reforzada para los datos genéticos de tal manera que su regulación «especial» quedaba relegada al concepto de «dato relativo a la salud» pero solo en la medida en que su análisis interferiría con la salud del individuo.[146] En esta fase embrionaria, la información[147] podía remitirse a Europol en el respeto del derecho nacional[148] de forma estructurada o no, pero las normas para su utilización, supresión o destrucción, incluidas las posibles restricciones de acceso, eran predeterminada por parte del Estado miembro remitente.[149] Los Estados miembros —pero no los países terceros de cuyos datos respondía siempre Europol— eran responsables de los datos transmitidos hasta su inclusión en el FTA, o incluso después, si Europol hubiese llegado a excluir su inserción por ser inexactos o no actuales.[150] En el caso de su inclusión, en cambio, los datos habrían sido procesados por Europol, indicando la(s) categoría(s) de personas afectadas,[151] «[…] en la medida en que [fuesen] adecuados, fieles, pertinentes y no excesivos respecto al objetivo del fichero de trabajo de análisis en que estén incluidos y siempre que no estén almacenados más tiempo del necesario para ese objetivo».[152] La conservación de los datos en un FTA debía revisarse con periodicidad anual y su supresión dependía del derecho nacional —p.e., la conclusión de la investigación subyacente, una sentencia judicial firme etc.; pero se estableció el límite máximo de tres años, o cinco en el caso de que surgiesen nuevos acontecimientos.[153] Además, la información se clasificaría según el grado de exactitud o fiabilidad, opiniones, o apreciaciones personales.[154] En el caso de que la información de un fichero hubiese sido relevante para otros ficheros, estos habrían podido ser interconectados mediante la creación de un nuevo fichero, o se podría transferir la información de uno al otro.[155] Además, el Protocolo del Convenio Europol del 6 de enero de 2004 introdujo un art. 6 bis para que Europol tratase la información cedida por los Estados miembros con el propósito de averiguar su pertinencia respecto a su mandato, y así introducirlos en el SIE.[156] Las normas para el tratamiento de estos datos habrían debido ser decididas por el Consejo de Administración de Europol, pero en ningún caso el límite máximo de conservación habría podido superar los seis meses.[157]

---

145 Art. 10 del Acto del Consejo de 3 de noviembre de 1998. Los FTA podían ser de naturaleza general o estratégica de cara a un problema particular, u operativa respecto a un caso, persona u organización.

146 A favor de una protección peculiar para los datos genéticos sensibles no relativos a la salud era ya Nicolás Jiménez *cit.* nota n.º 21, p. 81.

147 Art. 6 del Acto del Consejo de 3 de noviembre de 1998; el art. 6.1 menciona la «Información sobre identificación forense, como impresiones dactilares, resultados de la evaluación del ADN (únicamente con fines de identificación y sin información que caracterice la personalidad), características de la voz, grupo sanguíneo, información dental».

148 Art. 10.3 del Convenio Europol.

149 Art. 3.1 del Convenio Europol.

150 Art. 3.3 del Acto del Consejo de 3 de noviembre de 1998.

151 Art. 6.1 del Acto del Consejo de 3 de noviembre de 1998: «Siempre que se almacenen datos personales en ficheros de trabajo con fines de análisis deberá añadirse una nota que indique la categoría de personas dentro de la cual se almacenan».

152 Art. 4.1 del Acto del Consejo de 3 de noviembre de 1998.

153 Art. 7 del Acto del Consejo de 3 de noviembre de 1998.

154 Arts. 9 y 11 del Acto del Consejo de 3 de noviembre de 1998.

155 Art. 16 del Acto del Consejo de 3 de noviembre de 1998.

156 Protocolo establecido sobre la base del apartado 1 del artículo 43 del Convenio por el que se crea una Oficina Europea de Policía (Convenio Europol) por el que se modifica el mencionado Convenio, DOUE C 2 de 6.1.2004, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1713974389034&uri=CELEX%3A42004A0106%2801%29 [última consulta el 20 de abril de 2024].

157 Decisión del Consejo de Administración de Europol, de 20 de marzo de 2007, sobre los mecanismos de control de las consultas en el sistema informatizado de recogida de información, DOUE C 72 de 29.3.2007, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1713974389034&uri=CELEX%3A32007D0329%2801%29 [última consulta el 20 de abril de 2024].

La Decisión del Consejo de 2009, que convirtió a Europol en una agencia de la Unión bajo el tercer pilar,[158] autorizó el tratamiento de los datos genéticos de los sospechosos por haber cometido un delito, o de quienes se presumía que lo habrían cometido, y de los criminales de competencia de Europol en su art. 12.2, let. g).[159] En efecto, el art. 14.1 prohibía el tratamiento de los datos personales que revelasen «[…] el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas o la afiliación sindical, o el tratamiento de datos relacionados con la salud o la vida sexual […] salvo cuando sea estrictamente necesario para la finalidad del fichero de que se trate y a menos que tales datos completen otros datos personales introducidos en ese mismo fichero».[160] También se añadió la prohibición de seleccionar una categoría particular de personas a partir únicamente de los «datos sensibles»[161] mencionados. Sin embargo, aún no se mencionaban los datos genéticos y su procesamiento, dirigido a la identificación de criminales y terroristas, seguía rigiéndose por las disposiciones generales de protección de los datos con carácter personal. La Decisión del Consejo de 2009 mantuvo la distinción entre ficheros de análisis para el «tratamiento o utilización de datos para facilitar investigaciones penales»[162] y los ficheros de tipo general y estratégico, pero extendió el periodo de almacenamiento a tres años, prorrogables por otros tres.[163] Además, la supresión no procedía en el caso de perjudicar a intereses dignos de protección de la persona.[164] Si bien en un principio el uso de los datos de Europol habría debido limitarse a prevenir y combatir los delitos de competencia de Europol y las demás formas graves de delincuencia, estos habrían podido ser ulteriormente tratados para un fin distinto, o una autoridad diferente que las inicialmente competentes, bajo dos condiciones: 1ª La autorización previa del Estado transmitente, y 2ª El respeto del derecho nacional. En cualquier caso, la organización de los perfiles de ADN en el SIE no era comparable con la utilizada a nivel nacional por los Estados miembros: ni para realizar búsquedas rutinarias, ni para recibir entradas masivas de datos. Por el contrario, «DNA profiles are one element in the repertoire of "identification means" which objectively differentiate individuals from one another and assure self-sameness over time —necessary features of any intelligence database made up of case files on particular individuals».[165]

4.2. El procesamiento de perfiles de ADN en el mandato de Europol y su enmienda

El Anexo II del Reglamento 2016/794 confirmó la inclusión de los perfiles de ADN (parte no codificante) dentro de las categorías de datos personales procesables en el entorno informático de Europol[166] y, fi-

---

158 De Moor, Alexandra «The European Council Decision: Transforming Europol into an Agency of the European Union», *Common Market Law Review*, Vol. 47, n.º 4, 2010, pp. 1089-1121.

159 Art. 12.2, let. g) de la Decisión del Consejo de 6 de abril de 2009: «en la medida en que sea necesario, otras características que puedan resultar útiles para su identificación, en particular rasgos físicos específicos, objetivos y permanentes, tales como los datos dactiloscópicos y el perfil de ADN (establecido a partir de la parte no codificante del ADN)».

160 Art. 10.3 de la Decisión del Consejo de 6 de abril de 2009. Los datos personales contenidos en los FTA están enumerados en el art. 6 de la Decisión del Consejo de 6 de abril de 2009.

161 El término «dato sensible» se usaba, en aquel entonces, de forma impropia para indicar a unos datos de carácter personal que deberían de gozar de unas peculiaridades regulatorias tal y como señalaba Nicolás Jiménez, *cit.* nota n.º 21, p. 71.

162 Art. 14.2 de la Decisión del Consejo de 6 de abril de 2009.

163 Art. 16.3 de la Decisión del Consejo de 6 de abril de 2009.

164 Ar. 20.4 de la Decisión del Consejo de 6 de abril de 2009.

165 Johnson y Williams *cit.* nota n.º 140, p. 109.

166 A favor y en contra, respectivamente, de un régimen específico para los datos genéticos son Miño Vásquez, Verónica Gabriela «La protección de datos genéticos en virtud del Reglamento General de Protección de Datos», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º 51, 2019, pp. 77-90 y Martani, Andrea, Darryl Geneviève, Lester, Pauli-Magnus, Christiane, McLennan, Stuart, y Simone Elger, Bernice «Regulating the Secondary Use of Data for Research: Arguments Against Genetic Exceptionalism», *Frontiers in Genetics*, Vol. 10, n.º 1254, 2019, pp. 1-11.

nalmente, mencionó a los datos genéticos dentro de las categorías especiales de datos personales en su art. 30.2.[167] Según el art. 3 punto 17 del RPDUE, al que el mandato de Europol se remite, son datos genéticos los «datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona». En los primeros tiempos de su descubrimiento se pensaría que el ADN (parte no codificante), al no contener proteínas, no revelaría información sobre la fisiología o salud de la persona, por lo que sería asimilable a un «código a barra»[168] o una «huella genética» dentro de la definición amplia de biometría.[169] Sin embargo, esta diferenciación hoy se relativiza, pues, el perseguimiento de la finalidad identificativa por la que se procesan datos genéticos no privaría el ADN no codificante de su carácter sensible. Frente a quienes excluyen cualquier vulneración del derecho a la intimidad,[170] Nicolás Jiménez advierte[171] que el ADN no codificante puede relevar información muy precisa sobre la persona como, por ejemplo, el origen étnico, la existencia de enfermedades[172] o rasgos fenotípicos.[173] En definitiva, también el procesamiento del ADN no codificante debe considerarse una práctica muy invasiva en las esferas de la intimidad de la persona y requiere la previsión de un régimen de protección reforzado. Además, la definición de dato genético del RPDUE podría interpretarse en el sentido de excluir los perfiles de ADN no codificante del ámbito de aplicación del art. 30.2 del Reglamento Europol,[174] pero el régimen reforzado de las categorías especiales de datos personales podría aplicarse igualmente en virtud de la definición de «datos personales que revelen el origen étnico o racial» o «datos biométricos destinados a identificar de manera unívoca a una persona física».[175] De hecho, el Reglamento 2018/1862 incluye el perfil de ADN entre los ejemplos de datos biométricos,[176] y el Reglamento de Prüm II incluye dentro de la definición de dato biométrico los perfiles ADN, los datos dactiloscópicos, y las imágenes faciales.[177]

El art. 30 del Reglamento 2016/794 ha sido emendado por el Reglamento 2022/991 de forma significativa, si bien haya pasado algo desapercibido frente al más llamativo escándalo de los macrodatos. En su versión originaria, el art. 30.2 prohibía el tratamiento, automatizado o de otro tipo, de categorías especiales de datos personales «a menos que sea estrictamente necesario y proporcionado para la prevención o

---

167 El que corresponde al art. 9.1 del RGPD y al art. 10 DPDP. Solamente recientemente Europol ha sustituido referencias a la religión o a la conversión de las personas con la más amplia referencia a las «categorías especiales de datos personales»; cfr. el documento Europol, *Annual report on sensitive data – December 2019*, EDOC 924388, La Haya, 18 de diciembre de 2019 [documento divulgado el 7 de junio de 2024].

168 García y Alonso *cit.* nota n.º 28, p. 29.

169 Malanda, Sergio y Romeo Casabona, Carlos María *La identificación del ADN en el Sistema de Justicia Penal*, Thomson Reuters Aranzadi, Pamplona, 2010, p. 29, la definen como «el conjunto de técnicas y procedimientos automatizados de identificación y verificación individual de las personas por medios de sus características biológicas

170 Cfr. el preámbulo de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN (LO de datos policial), *BOE* n.º 242, de 9 de octubre 10 de 2007, disponible en: https://www.boe.es/buscar/act.php?id=*BOE*-A-2007-17634 [última consulta el 20 de abril de 2024].

171 Nicolás Jiménez *cit.* nota n.º 141, p. 1433.

172 Romeo Casabona, Carlos María «Datos biométricos (Comentario al artículo 4.14 RGPD)» Troncoso Reigada, Antonio (Ed) *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo I, Thomson Reuters Aranzadi, Pamplona, pp. 709-714, p. 700.

173 Gabrielle, Samuel y Prainsack, Barbara *The regulatory landscape of forensic DNA phenotyping in Europe VISAGE*, King's College London, Londres, 2018, p. 15.

174 Cfr. *mutatis mutandis* sobre la DPDP Kuru, Taner «C-205/21 *VS v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnoost*: Indiscriminate and Generalised Collection of Biometric and Genetic Data by law Enforcement Authorities in the EU Is Not Allowed», *European Data Protection Law*, Vol. 10, n.º 2, 2024, pp. 223-231, p. 228.

175 Art. 3 punto 18 del RPDUE.

176 Art. 3 punto 12 del Reglamento 2018/1862.

177 Art. 4.15 del Reglamento Prüm II.

la lucha contra los delitos enunciados en los objetivos de Europol y si esos datos complementan otros datos personales tratados por Europol». En su nueva formulación, en cambio, el art. 30.2 considera que dicho tratamiento «estará permitido solo cuando sea estrictamente necesario y proporcionado para fines de proyectos de investigación e innovación en virtud del artículo 33 bis y con fines operativos, dentro de los objetivos de Europol, y únicamente para prevenir o combatir los delitos que se incluyan en los objetivos de Europol». Por consiguiente, y en línea con el art. 10 de la DPDP, el tratamiento de categorías especiales de datos personales por Europol no está vetado, pero sí sigue sujeto a unas garantías específicas, que contemplan:

— el procesamiento de datos personales adicionales, en línea con el cdo. 37 de la DPDP, excepto en el caso de procesar los datos biométricos con el objetivo de identificar de forma univoca a una persona natural;[178]
— el respeto de los principios de estricta necesidad y proporcionalidad;[179]
— la prohibición de seleccionar a un grupo particular de personas sobre la base de estas categorías de datos solamente;
— el deber de informar al responsable de la protección de datos;[180]
— la imposición de un límite de acceso a los datos por algunos miembros del personal de Europol,[181] aunque excepcionalmente podría autorizarse el acceso a las autoridades competentes de los Estados miembros o los organismos de la Unión;[182] y
— la prohibición de transferir los datos a menos que resulte obligatorio por el Derecho UE y sea estrictamente necesaria y proporcionada en casos concretos de delitos comprendidos en los objetivos de Europol.[183]

A esta altura resulta relevante la sistematización del ADN (parte no codificante) dentro de la definición de dato genético o no: en este segundo supuesto, y siempre y cuando la finalidad perseguida sea la identificación univoca de la persona, el tratamiento de perfiles de ADN podría realizarse sin la necesidad de datos personales adicionales siguiendo al régimen más favorable aplicable a los datos biométricos. Además, en el caso de ejecutar análisis de *big data*, sobre lo que la normativa europea es aparentemente silenciosa,[184] Europol debe prestar atención a las normas sobre el procesamiento de datos a gran escala[185]

---

178 Grupo de Trabajo del Artículo 29, *Opinión n.º 3/2012 sobre la evolución de las tecnologías biométricas*, Bruselas, WP193, 27 de abril de 2012.

179 Sentencia del Tribunal de Justicia (Sala Quinta), *V.S.*, 26 de enero de 2023, ECLI:EU:C:2023:49. Refexiones sobre el concepto de «estricta necesidad» pueden encontrarse en Jasserand, Catherine «Processing of special categories of personal data» Kosta, Eleni y Bohem, Franziska (Eds) *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, pp. 217-230.

180 Art. 30.2 bis del Reglamento Europol.

181 Art. 30.3 del Reglamento Europol.

182 Art. 30.3, párrafo 2, del del Reglamento Europol, pero limitadamente a los casos previstos en el art. 20.1 y 2 bis, o para proyectos de investigación e innovación de conformidad con el art. 33 bis.2, let. d).

183 Art. 30.5 del Reglamento Europol.

184 Nicolás Jiménez, Pilar «Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/ Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext., 2019, pp. 129-167, p. 132, observa que el RGPD satisface el *big data* por ser «[…] fundamentado en unos principios generales y desarrollado a través de garantías que deben ser diseñadas para cada modelo de tratamiento». Para una crítica de la DPDP, en cambio, véase Vogiatzoglou, Plixavra y Marquenie, Thomas *Assessment of the implementation of the Law Enforcement Directive*, Estudio para la Comisión LIBE, Bruselas, 2022, p. 42, disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf [última consulta el 15 de septiembre de 2024].

185 Art. 39.3, let. b) del RPDUE y Alkorta Idiakez, Itziar «Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Bigdata», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext. 1, 2019, pp. 273-323, p. 285 y ss.

que requieren, por ejemplo, la elaboración de una evaluación de impacto relativa a la protección de datos personales (EIPD).[186] La EIPD es obligatoria, de acuerdo con el RGPD y la DPDP, para el responsable del tratamiento cuando el procesamiento entrañaría un alto riesgo en los derechos y libertades de los interesados, tomando nota de la naturaleza, ámbito, contexto y objetivos del tratamiento, por ejemplo, porque se efectúa mediante nuevas tecnologías aplicadas a gran escala o que hacen más difícil el ejercicio de los derechos individuales por parte de los interesados.[187] Según el Grupo de Trabajo del Artículo 29, el tratamiento de categorías especiales de datos personales entrañaría siempre un riesgo de discriminación o de perjudicar significativamente al individuo, con independencia de la técnica de procesamiento que se utilice;[188] por su parte, la Agencia Española de Protección de Datos (AEPD) incluye dentro de las operaciones de alto riesgo las categorías especiales de datos y la información que, indirectamente, esté relacionada con dichas categorías así como el uso de datos genéticos para cualquier fin.[189] Sin embargo, se podría prescindir de la EIPD cuando el tratamiento se base en una obligación legal, una misión de interés público, o en el ejercicio de poderes públicos y la EIPD se haya realizado en el contexto de la adopción de dicha base jurídica.[190] En el caso de Europol, competiría[191] a la propia Agencia realizar la EIPD de las operaciones de tratamiento de los datos operativos[192] bajo la supervisión del responsable de protección de datos.[193] El mandato de la Agencia sigue al art. 35.1 *in fine* del RGPD al prever que una EIPD puede cubrir operaciones de tratamientos similares que presentan riesgos similares, pero esta previsión podría confundirse, a nuestro juicio, con la del art. 39.1 del Reglamento Europol por el que «[…] la consulta previa al SEPD no se aplicará a actividades operativas específicas que no incluyan ningún **tipo nuevo de tratamiento** que implique un **riesgo elevado** para los derechos y libertades de los interesados».[194] Estos dos artículos se aplican cumulativamente (es decir, el responsable del procesamiento no tiene la obligación de realizar una EIPD y, a la vez, no debe consultar previamente al SEPD) solo cuando el nuevo tipo de tratamiento es similar a otro y los dos constituyen unos riesgos elevados similares. No obstante, el Reglamento Europol no ofrece una definición de «tipo nuevo de tratamiento», expresión que podría terminar asimilándose, por ejemplo, a la de «ulterior tratamiento», siendo esta última más clara y fácilmente interpretable como hemos visto en más arriba. En cualquier caso, y siempre que se trate de categorías especiales de datos personales, no vendría menos el deber del responsable de la operación de informar al responsable de la protección de datos que, en última instancia, responde ante el SEPD en virtud del art. 41 ter.1, let. h) del Reglamento Europol. Finalmente, quedaría a cargo de Europol sopesar el riesgo de *output* incorrectos o prejudiciales, i.e. discriminatorios,[195] en virtud del principio de la calidad de los datos,[196] así como la necesidad de engullir una cantidad de información mínima indispensable para la consecución de sus objetivos en consideración del Anexo II adjunto a su mandato. En efecto, el art. 30.2 del Reglamento Europol debe leerse como una disposición adicional respecto a los principios y normas generales que protegen

---

186 Grupo de Trabajo del Art. 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruselas, 4 de abril de 2017.

187 Art. 35.1 del RGPD y art. 27 de la DPDP.

188 Grupo de trabajo del artículo 29, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680),* WP 258, Bruselas, 2017, p. 8.

189 AEPD, *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos*, Madrid, 2023, p. 2.

190 Art. 35.10 del RGPD.

191 Art. 38.4 del Reglamento Europol, la negrita es nuestra.

192 Art. 89.1 del RPDUE.

193 Art. 41 ter.1, let. c) del RPDUE.

194 Art. 39 del Reglamento Europol.

195 Kusak, Martyna «Quality of data sets that feed AI and big data applications for law enforcement», *ERA Forum*, n.º 23. 2022, pp. 209-219.

196 Art. 71.1, let. d) del RPDUE.

el tratamiento de los demás datos personales, como el de la licitud y legalidad del tratamiento,[197] o el de la limitación de la finalidad perseguida.[198] Por consiguiente, el tratamiento de los perfiles de ADN (parte no codificante) deberá siempre justificarse a la luz de los límites competenciales que hemos analizado anteriormente,[199] con la salvedad del principio de la finalidad del tratamiento que sigue unas pautas propias tal y como pasamos a analizar a continuación.

4.3. Las finalidades por las que Europol puede (re)procesar los perfiles de ADN

El art. 30.2 del Reglamento Europol blinda los supuestos en los que Europol puede procesar categorías especiales de datos personales a dos hipótesis:

1. para los proyectos de investigación e innovación,[200] y
2. para la finalidad operativa de apoyo a la cooperación entre autoridades policiales de la Unión.[201]

Si bien no se detalla, entendemos que la delimitación funcional prevista por el art. 30 del Reglamento Europol se aplica tanto al uso primario de las categorías especiales de datos personales como al uso ulterior de estos y que, en este último caso, el art. 30.2 debe leerse junto al art. 19 del Reglamento Europol respecto a la determinación de los fines y las restricciones del tratamiento.[202] En este sentido, excluimos la posibilidad de que Europol procese los perfiles de ADN para los análisis estratégicos o temáticos, o para informar al público sobre las personas sospechosas o las condenadas en búsqueda de una resolución judicial, aunque estas tareas se contemplen en el art. 18.2 del Reglamento Europol.[203]

4.3.1. El tratamiento de categorías especiales de datos personales para la finalidad operativa

Incierto es el alcance de la «finalidad operativa» mencionada en segunda instancia por el art. 30.2 del Reglamento Europol, pues esta expresión no coincide con la definición de «análisis operativo» prevista por el art. 2, let. c) de este mismo Reglamento. El enfoque funcional escogido por los co-legisladores[204] podría comprender un abanico de tareas muy amplio, que va desde el procesamiento de categorías especiales de datos en virtud del art. 18.2, let. c) del Reglamento Europol, hasta la capacidad de Europol para coordinar, organizar y ejecutar acciones operativas y de investigación.[205] El primero, el análisis operativo, consiste en «todos los métodos y técnicas mediante los cuales la información se recopila, almacena, trata y evalúa con la finalidad de apoyar investigaciones penales»[206] y se realiza mediante un PA (Proyectos de Análisis) operativo del que debe ser informado el Consejo de Administración de Europol y el SEPD.[207] Cada

197 Art. 72 del RPDUE.
198 Art. 71.1, let. b) del RPDUE.
199 Art. 72 del RPDUE.
200 Art. 33 bis del Reglamento Europol.
201 Arts. 1 y 3 del Reglamento Europol.
202 Cfr. nuestro análisis en el epígrafe 3.2.
203 Art. 18.2, lets. b) y f) del Reglamento Europol.
204 Coudert, Fanny «The Europol Regulation and Purpose Limitation: From the "Silo-Based Approach" to What…Exactly?», *European Data Protection law Review*, Vol. 3, n.º 3, 2017, pp. 313-324.
205 Art. 88.2, let b), del TFUE.
206 Art. 2, let. c), del Reglamento Europol.
207 Art. 18.3, let. a) del Reglamento Europol.

PA operativo debe especificar el objetivo perseguido, las categorías de datos personales y de interesados, los participantes, la duración de la conservación y condiciones de acceso, transferencia y uso de los datos en cuestión.[208] La segunda, la actividad operativa, ha sido consagrada en el propio TFUE que hace alusión a los Equipos Conjuntos de Investigación de forma ejemplificativa.[209] A tal efecto, recordamos que Europol ha venido desplegando sus funcionarios en los *hotspots* para la lucha contra el tráfico ilícito de migrantes y la trata de seres humanos[210] y la Propuesta de Reglamento presentada el pasado noviembre 2023 potenciará la capacidad de Europol para procesar datos biométricos mediante técnicas de reconocimiento facial, y para analizar los perfiles de ADN aptos a la identificación de las víctimas y de las redes criminales subyacentes.[211]

Con todo, de la formulación del art. 30.2 del Reglamento Europol se desprende que el legislador de la UE no ha querido limitar el uso de las categorías especiales de datos personales al «análisis operativo» sino que se ha dejado un margen de apreciación más amplio de cara a las ulteriores tareas «operativas» que Europol puede desarrollar. Dentro de estas tareas entrarían, por ejemplo, los controles cruzados de datos y la facilitación del intercambio de información entre autoridades. Se recuerda, en este sentido, que el RPDUE aporta una definición amplia de «datos personales operativos» entendidos como «todos los datos personales tratados por los órganos u organismos de la Unión cuando lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE a fin de realizar los objetivos y funciones establecidos en los actos jurídicos por los que se crean dichos órganos u organismos».[212] A nuestro juicio, los co-legisladores habrían podido conferir mayor seguridad al procesamiento de las categorías especiales de datos personales (incluidos los perfiles de ADN) haciendo mención expresa de todas o algunas de las tareas previstas por el art. 18.2 del Reglamento Europol.

4.3.2. El tratamiento de categorías especiales de datos personales para fines de investigación e innovación

El tratamiento de datos personales para fines de investigación e innovación es una nueva tarea atribuida a Europol por las enmiendas de 2022.[213] Esta disposición está destinada a adquirir gran relevancia en el contexto securitario de cara a la experimentación de nuevas tecnologías de aprendizaje automatizado[214] basa-

---

208 Art. 18.3, let. a) del Reglamento Europol, sobre el uso secundario cfr. *supra*.

209 Cfr. el art. 7 del Reglamento (UE) 2023/969 del Parlamento Europeo y del Consejo 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 DOUE L 132 de 17.5.2023, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32023R0969 [última consulta el 20 de abril de 2024].

210 Fernández Rojo, David «La declaración de la víctima de tráfico ilegal de migrantes como prueba preconstituida y las corroboraciones externas que han de reforzar su verosimilitud», *Revista de Derecho Comunitario Europeo*, n.º 123, pp. 65-98.

211 Lorente, José A., Saiz, María, Haarkötter, Christian, Robles-Fernández, Inmaculada, Álvarez-Cubero, María, Gálvez, Xiomara, Martínez-González, Luis J., Lorente-Remón, Begoña, C. Álvarez, Juan, «Genetic identification against traffic in human beings», *Forensic Science*, 2020, pp. 1-13.

212 Art. 3.2 del RPDUE.

213 Art. 4.1, lett. v) y w), art. 4.4 bis, y art. 18.2, let. e) del Reglamento Europol. En 2023, Europol no procesó ningún dato personal para fines de investigación e innovación según el documento de Europol, *Annual Reporting to EDPS on Art. 30 and 31 of the ER*, EDOC 1256980, La Haya, 8 de diciembre de 2023 [documento divulgado el 7 de junio de 2024].

214 Comisión Europea, *Artificial Intelligence for Europe,* COM(2018) 237 final, Bruselas*,* 25.4.2018*,* p. 10 disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN [última consulta el 20 de abril de 2024]: «*Machine learning, a type of AI, works by identifying patterns in available data and then applying the knowledge to new data.35 The larger a data set, the better even subtle relations in the data can be discovered*».

das en el *big data*[215] y la IA.[216] Recientemente, Europol ha puesto en marcha un propio laboratorio para desarrollar, entrenar y validar modelos y herramientas de IA[217] y así suportar, por ejemplo, la implementación del Sistema de Información y Autorización de Viajes (SEIAV) y del Sistema de Información de Visados (VIS). El Laboratorio de Innovación de Europol establecerá y pondrá a disposición de los Estados miembros una *sandbox*[218] llamada ODIN (*Operational Data for Innovation*) donde se ensayarán y refinarán algoritmos con datos «reales» u «operativos» a partir de la información de la que puede disponer la propia Agencia.[219] De acuerdo con el Consejo Ejecutivo de Europol, esta *R&I Sandbox* «will establish a legal and technical environment in which Europol and the MS competent authorities will be able to co-create, test, validate and refine innovation solutions with which to face operational challenges».[220]

Como es sabido, el RGPD establece una amplia flexibilidad en el caso de usar los datos personales a efectos de investigación científica,[221] lo que este instrumento interpreta de forma amplia como el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado.[222] Antes de todo, el RGPD permite que el titular de los datos personales preste su consentimiento en un sentido amplio,[223] o prescinde de este en el caso de retener ulteriormente los datos personales,[224] ya que el uso ulterior de los datos personales con fines de investigación científica se presume legalmente compatible.[225] Según Recuero Linares: «Significa, por tanto, que el responsable del tratamiento no necesitará una base jurídica distinta de la primigenia —fuese o no el consentimiento del interesado— que permitió la obtención de los datos personales si los va a destinar ulteriormente a la investigación científica».[226] La derogación al principio de la limitación de la finalidad matiza la imperatividad del

---

215 Barash, Mark, McNevin, Dennis, Fedorenko, Vladimir, Giverts, Pavel «Machine learning applications in forensic DNA profiling: A critical review», *Forensic Science International: Genetics*, Vol. 69, 2024, pp. 1-15, p. 5, se remiten expresamente al análisis por regresión y reducción de la dimensionalidad junto a los modelos de *machine learning* generativos.

216 Consejo de la UE, documento 9185/20 ADD 1, Bruselas, 8 de julio de 2020, p. 9, donde el Coordinador de la UE para la lucha contra el terrorismo propuso insertar una base específica en el mandato de las agencias del ELSJ para investigar, desarrollar, ensayar, auditar y validar herramientas de IA para la seguridad interna.

217 EU Innovation Lab for Internal Security, *EU Innovation Lab for Internal Security: Annual Report*, La Haya, 2022, disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Eu%20Innovation%20Hub%20Annual%20event%20report%202023.pdf [última consulta el 20 de abril de 2024].

218 Art. 57 del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial o simplemente RIA) DOUE L, 2024/1689, 12.7.2024, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL_202401689 [última consulta el 17 de septiembre de 2024].

219 Arts. 18 y 33 del Reglamento Europol y Europol, *ODIN (PD). Research & Innovation Sandbox (Personal Data Processing Environment). Use & Management Policy*, La Haya, 15 de febrero de 2024, disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Doc%203%20-%20EDOC%20-%231392061-v1-Public%20version%20of%20EDOC-%231327390.PDF [última consulta el 15 de septiembre de 2024].

220 Consejo de Administración, *Europol Innovation Law. Progress Report and Strategic Priorities 2024-2025*, La Haya, 22 de septiembre de 2023, p 1, disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC%231384018_Public_version_Redacted_of_EDOC%231321956v13_Innovation_Lab_MB_report_October_2023.pdf [última consulta el 20 de abril de 2024].

221 Mészáros, János y Ho, Chih-hsing, «The Big Data and Scientific Research: The Secondary Use of Personal Data under Research Exemption in the GDPR», *Hungarian Journal of Legal Studies*, Vol. 59, n.º 4, 2018, pp. 403-419.

222 Cdo. 159 del RGPD.

223 Cdo. 33 del RGPD.

224 Cdo. 65 del RGPD.

225 Art. 5.1, let. b) del RGPD.

226 Recuero Linares, Mikel *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectivas europeas ante el desafío globalizado*, AEPD, Madrid, 2019, p. 30.

consentimiento explicito, o individualizado, en el caso de procesar categorías especiales de datos personales también[227] por lo que concierne la individuación de la base jurídica que legitima el tratamiento de los datos, pero no a efectos del levantamiento de la prohibición del art. 9.1 del RGPD. En el supuesto de tratar categorías especiales de datos personales para fines de investigación científica, de hecho, el art. 9.2, let. j), del RGPD exige contar con una normativa específica aprobada por el legislador de la UE o de un Estado miembro; en su defecto, la prohibición del art. 9.1 del RGPD debería de levantarse sobre la base de otro de los supuestos previstos por el art. 9.2 del RGPD.

En el caso de Europol, la licitud del tratamiento de los datos operativos a afectos de investigación e innovación se justifica sobre la base del propio Reglamento Europol (art. 33 bis) al amparo del art. 88 del TFUE al que al art. 72 del RPDUE se remite.[228] A nuestro juicio, el procesamiento de datos de investigación e innovación por parte de Europol puede darse en dos hipótesis: 1.ª un «primer uso» de datos personales que Europol colecciona directamente o que los Estados miembros, los organismos de la Unión, los países terceros y organizaciones internacionales, y las partes privadas o los particulares, le hayan cedidos; y 2.ª un «uso ulterior» de datos personales que han sido procesados en primera instancia para fines operativos de conformidad con el art. 18.2, lets. a), b), c), d), y f) del Reglamento Europol.[229]

En el primer caso (primer uso respecto al mandato de Europol), y siguiendo a las reflexiones que hemos realizado en el epígrafe 3.2, el proveedor de la información debe poder contar con una base jurídica que le legitima coleccionar y ceder datos personales a efectos de investigación e innovación.[230] En este sentido, se ha observado[231] como la formulación del art. 9.1 y 2 de la DPDP sobre las condiciones específica del tratamiento de datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública por parte de las autoridades competentes,[232] podría resultar excesivamente estricta por exigir: primero, que la ley nacional habilite las autoridades competentes a desarrollar funciones no estrictamente policiales, como la investigación científica; segundo, cumplir con las disposiciones del RGPD; tercero, y en alternativa a una habilitación legal para el «primer uso», que la ley nacional permita a las autoridades competentes el uso ulterior de los datos originariamente procesados para finalidades policiales a efectos de investigación científica. En el caso de España, por ejemplo, el art. 2.3 de la Ley Orgánica 7/2021[233] excluye rotundamente de su ámbito de aplicación los tratamientos de datos personales «realizados por las autoridades competentes para fines distintos de los previs-

---

227 Art. 9.2, let. a) del Reglamento Europol.

228 Art. 33 bis.2, let. a) punto iv) del RPDUE.

229 Los co-legisladores no aclaran de donde proceden los datos que Europol podría procesar a efectos de investigación e innovación. Este se desprende de una lectura comprensiva del Reglamento Europol que pone de relieve la posibilidad del ulterior tratamiento de los datos procesados por la Agencia a efectos operativos, tal y como hemos estudiado más arriba.

230 Grupo de Trabajo de Gestión de la Información, *Building the Research and Innovation Pipeline. Update on the implementation of article 33.ª and the R&I Sandbox environment*, La Haya, 17 de abril de 2023, p 5, disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Doc%205%20-%20EDOC%20-%231392063-v1-Public%20version%20of%20EDOC-%231301551.PDF [última consulta el 15 de septiembre de 2024], y Sentencia del TJUE (Sala Quinta) *V. S. c. Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost,* 26 de enero de 2023, ECLI:EU:C:2023:49, párrafos 74-76.

231 Bolognini, Luca *A proposal for the EU privacy law simplification, supporting data-driven research in the law enforcement field*, Istituto Italiano per la privacy e la valorizzazione dei dati, 10 de enero de 2020, https://www.istitutoitalianoprivacy.it/2020/01/10/a-proposal-for-the-eu-law-simplification-supporting-data-driven-research-in-the-law-enforcement-field/ [última consulta el 15 de septiembre de 2024|.

232 Art. 3, punto 7) de la DPD.

233 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, *BOE* n.º 126, de 29 de mayo de

tos en el artículo 1, incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos». El art. 2.3 de la LOPDP añade que en estos casos se deben aplicar el RGPD y la Ley Orgánica 3/2018,[234] y la posibilidad de que las autoridades españolas competentes (listadas en el art. 4 de la LOPDP) desarrollen actividades distintas que las estrictamente policiales y, en concreto, que puedan procesar datos personales a efectos de investigación científica[235] se establece en el art. 6.4 de la Ley Orgánica 7/2021. Por tanto, las autoridades españolas competentes (sean estas u otros designadas como responsables del tratamiento) han sido empoderada legalmente para usar los datos policiales a efectos científico, estadístico o histórico. En estos casos, se deberán aplicar unas «garantías adecuadas para los derechos y libertades de los interesados» de conformidad con las normas del RGPD que hemos señalado más arriba.

En el segundo caso (uso ulterior respecto al mandato de Europol), el Reglamento Europol prevé disposiciones contradictorias: por un lado, el art. 33 bis.5 establece que Europol debe solicitar el consentimiento del proveedor de la información *ex post*, de conformidad con el art. 19.2 del Reglamento Europol;[236] por el otro lado, el art. 19.2, párrafo 4.º, permite que la información remitida a efectos del art. 18.2, lets. a), b), c), y d) del Reglamento Europol «[…] podrá ser tratada por Europol a efectos del artículo 18, apartado 2, letra e), de conformidad con el artículo 33 bis». El art. 33 bis.5 *in fine* reitera que «Europol no tratará datos para proyectos de investigación e innovación sin el consentimiento del proveedor de los datos» pero, a nuestro juicio, existe una incoherencia normativa interna que, en última instancia, permitiría a la Agencia (re)procesar los datos personales operativos cedidos al entorno de Europol sin necesidad del consentimiento del proveedor de los datos, con la única excepción del art. 18.2, let. f) del Reglamento Europol. Aunque no se especifique, creemos que el consentimiento del proveedor de los datos es indispensable para averiguar la compatibilidad del uso ulterior de la información cedida a Europol para fines de investigación e innovación respecto al derecho aplicable a la parte remitente; uso que, hemos adelantado, se presume compatible en el ordenamiento español en virtud del art. 5.1, let. b) del RGPD pero no en el caso de los datos policiales en virtud del art. 9.1 y 2 de la DPDP. En definitiva, el consentimiento del proveedor permite averiguar la existencia de una base jurídica, con rango de ley, que legitima el tratamiento ulterior de los datos personales policiales para fines de investigación e innovación de tal manera que, al delegar esta tarea a Europol, las autoridades competentes no puedan eludir las previsiones de derecho interno adoptadas por su Estado miembro.

Con independencia de si Europol procesa categorías especiales de datos personales para fines de investigación e innovación como primero o ulterior uso, el art. 33 bis.1 del Reglamento Europol impone a la Agencia dos condiciones principales a respetar: primero, que el tratamiento sea absolutamente necesario y esté debidamente justificado para lograr los objetivos del proyecto de que se trate y, segundo, y por lo que se refiere a las categorías especiales de datos personales precisamente, que el tratamiento sea estrictamente necesario y esté sujeto a unas garantías adecuadas,[237] entre las que se puede incluir la seudoni-

---

2021, disponible en: https://www.boe.es/buscar/act.php?id=*BOE*-A-2021-8806 [última consulta el 15 de septiembre de 2024] (LOPDP en adelante).

234 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, *BOE* n.º 294, de 6 de diciembre de 2018, disponible en: https://www.boe.es/buscar/act.php?id=*BOE*-A-2018-16673 [última consulta el 15 de septiembre de 2024] (LOPDGDD en adelante).

235 En el caso de los perfiles de ADN, por ejemplo, véase el art. 7 de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, *BOE* n.º 242, de 9 de octubre de 2007, disponible en: https://www.boe.es/buscar/act.php?id=*BOE*-A-2007-17634 [última consulta el 15 de septiembre de 2024].

236 Art. 33 bis.5 del Reglamento Europol.

237 Art. 89.1 del RGPD exigiría: una base legal en Derecho de la Unión o de los Estados miembros; el respeto del principio de proporcionalidad de cara al objetivo perseguido; el respeto de la esencia del derecho a la protección de datos, y la previsión de medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

mización.[238] A diferencia que el art. 89.1 del RGPD, por lo tanto, el Reglamento Europol no menciona ni el principio de la minimización de datos (i.e., datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados),[239] ni la opción de la anonimización «[s]iempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo». Recordamos que el proceso de disociación de los datos puede ser reversible (seudonimización) o irreversible (anonimización), dependiendo de la proporcionalidad del esfuerzo a realizar en términos de tiempo, gastos y trabajo.[240] En el caso de los datos genéticos, el procedimiento de disociación se implementa por codificación: a cada genotipo se atribuye un código de identificación separado de la información sobre la persona o indicio correspondiente.[241] Sin embargo, el esfuerzo de reidentificación se ha aliviado considerablemente a raíz del análisis del *big data* y del procesamiento a gran escala.[242] Tanto es así, que la vía de la anonimización ha sido cuestionada en la práctica.[243] Según Nicolás Jiménez, entonces, la disociación debe considerarse un test dinámico que se valoraría sobre la base del contexto, y de las garantías éticas aplicables. Haciendo hincapié en la seudonimización (a diferencia que la anonimización), el art. 33 bis del Reglamento Europol no sustrae el art. 33 bis de las garantías sobre la protección de los datos personales, si bien la Agencia esté persiguiendo fines de investigación e innovación.[244]

De ahí destacamos otro aspecto de interés: a diferencia que el art. 89.2 del RGPD que nos indica con precisión las garantías y excepciones aplicables a los derechos del titular de los datos personales que sean procesados con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, el art. 33 bis del Reglamento Europol no recuerda los derechos subjetivos (si bien restringibles) de información, acceso, rectificación y restricción del tratamiento que el titular debe poder ejercer.[245] Los arts. 36 y 37 del Reglamento Europol recogen los derechos de acceso, rectificación, y cancelación de los datos personales así como el derecho de restricción del procesamiento y otorgan el derecho a formular la solicitud correspondiente a la autoridad designada a tal efecto en los Estados miembros o ante Europol. La decisión resultante de la solicitud de acceso es fruto de la cooperación estrecha entre Europol, el proveedor de la in-

---

238 Art. 33 bis.1 del Reglamento Europol y art. 89.1 del RGPD.

239 Sobre la importancia del principio de la minimización de datos y la IA véase Lazcoz Moratinos, Guillermo *Gobernanza y supervisión humana de la toma de decisiones automatizada basada en la elaboración de perfiles,* Universidad del País Vasco (UPV/EHU), 2023, p. 105 y ss. El autor, p. 106, critica la propuesta de la Comisión Europea que permitiría procesar categorías especiales de datos personales para paliar los «sesgos algorítmicos»; razón por la que el actual cdo. 70 del RIA permite tratar categorías especiales de datos personales en los sistemas de IA de alto riesgo como cuestión de interés público esencial. Sobre los sesgos en la IA véase de Miguel Beriain, y Mursuli Yanes, Yenifer «Sesgos, IA y biomedicina: un comentario desde la ética del Derecho», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º 59, 2023, pp. 1134-7198.

240 Nicolás Jiménez, Pilar «Investigación con muestras biológicas y biobancos» Romeo Casabona, Carlos María (Ed) *Manual de bioderecho*, Dykinson, Madrid, 2022, p. 654 y ss.

241 Lorente Acosta, José Antonio «Identificación genética criminal: importancia médico legal de las bases de datos de ADN» Romeo Casabona, Carlos María (Ed) *Bases de datos de perfiles de ADN y criminalidad*, Comares, Granada, 2002, pp. 1-26, pp. 24 y 25.

242 Recuero Linares *cit.* nota n.º 228, p 10.

243 Philips, Mark «GDPR Brief: can genomic data be anonymised?» *Global Alliance for Genomics & Health*, 10 de octubre de 2018, disponible en: https://www.ga4gh.org/news_item/can-genomic-data-be-anonymised/ última consulta el 15 de septiembre de 2024].

244 Art. 4, punto 5), del RGPD.

245 Nicolás Jiménez *cit.* nota n.º 186, p. 152 y ss., pone de relieve que el derecho a la supresión de los datos personales no se menciona en el art. 89.2 del RGPD, pero su ejercicio puede inferirse del art. 17.3, let. d) del RGPD que circunscribe esta excepción cuando la obligación de información «pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento».

formación, así como los Estados miembros afectados[246] y, en el caso de que la rectificación o cancelación proceda, el proveedor de la información (cuando lo haya) deberá a su vez rectificar o cancelar dichos datos.[247] Sin embargo, el Reglamento Europol no impone a la Agencia (en calidad de responsable de la protección de datos)[248] informar al interesado, derecho trascendental «en tanto a través del mismo se permite ejercitar otros».[249] Este deber debería extraerse, en nuestra opinión, del art. 79 del RPDUE, pues, es difícil de esperar que el interesado consiga solicitar el acceso, la rectificación y (posiblemente) la supresión de sus datos personales[250] a falta del recibir información sobre el tratamiento. Siguiendo al art. 79.3 del RPDUE, el deber de información se debe garantizar también en el marco de la cooperación policial y judicial penal, pudiéndose retrasar, limitar u omitir en el respeto de los principios de necesidad y proporcionalidad en una sociedad democrática. La no previsión del deber de Europol de informar al interesado es, por tanto, cuestionable y necesitaría de una inspección más profundizada de cara a la aplicación y respeto del principio de transparencia en el contexto policial. Sin embargo, en el caso de tratar los datos personales a efectos de investigación e innovación al amparo del RGPD, los requisitos legales podrían ser diferentes. En efecto, el cdo. 62 del RGPD, permite *glisser* la obligación de información «cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado», en particular, cuando «el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos».

El art. 33 bis.1 *in fine* exige que el tratamiento respete los principios de transparencia, explicabilidad, equidad y rendición de cuentas. El art. 33 bis.2 del Reglamento Europol impone a la Agencia recaudar la autorización del director ejecutivo sobre cada proyecto de investigación e innovación. Luego, Europol debe consultar al responsable de la protección de datos y al agente de derechos fundamentales. El responsable de protección de datos[251] no debe confundirse con el responsable del tratamiento de los datos, cuestión que se elucidaría sobre la base de la persona que decide la finalidad y los medios del tratamiento. Entendemos que estos criterios serán determinados en el seno del Consejo de Administración de Europol que reúne a un representante de cada Estado miembro y un representante de la Comisión Europea.[252] Puesto que los datos personales por tratar en el contexto de un proyecto de investigación e innovación deben copiarse en un entorno separado, aislado, y protegido, con acceso limitado garantizado solo al personal de Europol,[253] las autoridades de los Estados miembros, y el personal de la Unión establecido sobre la base del título V del TFUE, Europol podrá decidir si ceder la ejecución del proyecto a un proveedor (privado) externo que figuraría como encargado del tratamiento.[254] En concreto, la autorización del director ejecutivo sobre el proyecto de investigación e innovación deberá avalar los siguientes extremos:

---

246 Art. 36.5 del Reglamento Europol.

247 Art. 37.4 y 5 del Reglamento Europol.

248 El art. 38.2, let. b) del Reglamento Europol limita la responsabilidad de Europol sobre la exactitud de los datos personales «facilitados por países terceros u organizaciones internacionales o directamente por entidades privadas, por los datos personales extraídos por Europol de fuentes públicas o que resulten de los propios análisis de Europol y por los datos personales almacenados por Europol». En los demás casos (Estados miembros u organismos de la Unión que facilitan los datos personales) competiría al proveedor de la información cumplir con dicha obligación; cfr. por ejemplo el art. 13 de la DPDP en lo que respecta al tratamiento de datos personales por las autoridades competentes designadas por los Estados miembros.

249 Nicolás Jiménez *cit.* nota n.º 21, p. 186.

250 En la Sentencia del Tribunal de Justicia (Gran Sala), *Kočner c Europol,* de 5 de marzo de 2024, ECLI:EU:C:2024:202, por ejemplo, el recurrente conoció del procesamiento (ilícito) de sus datos personales a causa de la publicación en la prensa y en Internet.

251 Art. 41 del Reglamento Europol.

252 Art. 10 del Reglamento Europol.

253 El concepto de «entorno seguro» será desarrollado bajo el nuevo Reglamento sobre el Espacio Europeo de Datos Sanitarios que hemos citado más arriba.

254 Art. 3, punto 12) del RPDUE.

— la descripción de los objetivos del proyecto, y la justificación de su relevancia para el sector policial, así como la explicación de su utilidad para Europol o las autoridades nacionales;[255]
— la descripción de la actividad de tratamiento prevista que comprendería la exposición de los objetivos, el alcance y la duración del tratamiento, y la necesidad y proporcionalidad del tratamiento de datos personales;
— la descripción de las categorías de datos personales y (añadiríamos) de las categorías especiales de datos personales que se tratarían;
— la valoración de la licitud del tratamiento de datos personales operativos, el plazo de conservación y las condiciones de acceso a los datos;
— la EIPD, lo que incluye una valoración del riesgo sobre los derechos de los interesados, de sesgos en los datos personales y en el resultado del tratamiento, así como las medidas de mitigación.

Otra diferencia más entre el art. 33 bis del Reglamento Europol y el RGPD es la prohibición de que la actividad de investigación e innovación de Europol pueda dar lugar a medidas o decisiones que afecten a los interesados como resultado del tratamiento. Dicho con otras palabras, se prohíbe la generación de inferencias (p.e. decisiones) sobre los particulares a raíz de los ensayos, con independencia del beneficio o perjuicio que estas puedan ocasionar. Esta matización nos distancia del contexto experimental de los datos de salud, pues, siguiendo al RGPD las medidas beneficiosas que se pueden descubrir de una investigación científica deben poderse aplicar al paciente.[256] Parece, entonces, que los co-legisladores han querido evitar caer en las mallas de la prohibición de las decisiones basadas únicamente en el tratamiento automatizado del art. 22 del RGPD;[257] disposición, además, que no queda reflejada en el Reglamento Europol. En el mismo sentido, el art. 33 bis se quedaría al margen del RIA que en su art. 2.6 establece: «El presente Reglamento no se aplicará a los sistemas o modelos de IA, incluidos sus resultados de salida, desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad». De un modo opuesto, Europol se compromete a difundir sus resultados para crear sinergias entre las actividades de investigación e innovación de los correspondientes organismos de la Unión.[258]

Last but not least, el tratamiento de datos personales a efectos de investigación e innovación (cuya retención puede alargarse más allá de la ejecución de un proyecto específico) está sometido a un proceso de rendición de cuentas, en virtud del cual Europol debe:

— remitir información al SEPD sobre el inicio del proyecto;
— consultar o informar al Consejo de Administración antes del inicio del proyecto;[259]
— implementar medidas de seguridad y de protección de datos a lo largo del proyecto, y
— conservar registros sobre el tratamiento de datos personales en el contexto del proyecto durante dos años.

El Consejo de Administración de Europol remite sucesivamente un documento vinculante sobre el alcance general de estos proyectos al SEPD. Además, Europol deberá documentar la justificación del entrenamiento, prueba y validación de los algoritmos para garantizar la transparencia en el proceso y la exactitud de los resultados alcanzados. Estos documentos podrán ser puestos a disposición de las partes interesadas, los Esta-

---

255 En Europol *cit.* nota n.º 221, p. 8 se específica que el proyecto debe dar lugar a resultados tangibles, aunque estos sean negativos; además el proyecto no debe suponer riesgos o infracciones inaceptables de los derechos humanos.

256 Cdo. 159 *in fine* del RGPD, y Nicolás Jiménez *cit.* nota n.º 186, p. 156: «[…] el posible beneficio directo para la salud que se pudiera derivar de los resultados de la investigación, hace nacer una obligación para los investigadores que desarrollan una actividad en un contexto diferente al asistencial, con otras reglas y requisitos».

257 Lazcoz Moratinos *cit.* nota n.º 241.

258 Art. 4.4 bis del Reglamento Europol.

259 Art. 18.7 del Reglamento Europol.

dos miembros, y el Grupo de Control Parlamentario Conjunto.[260] En ningún caso, los datos personales que vayan a tratarse en el contexto de un proyecto no pueden «transmitirse» o «transferirse»; expresiones que (a nuestro entender) quieren impedir que los datos dejen el entorno físico en el que son procesados pero no prohíben el acceso a los mismos por parte de organismos de la Unión, terceros países y organizaciones internacionales, tal y como nos proponemos de estudiar en el futuro.

5. Conclusiones

Europol es el eje de información de la UE para la prevención y lucha contra crímenes graves transnacionales y el terrorismo. Su competencia analítica ha sido considerablemente reforzada tras la entrada en vigor del Tratado de Lisboa y, a raíz del Reglamento 2016/679, Europol dispone de un nuevo entorno informático que permite el análisis de macrodatos apoyado en el concepto de interoperabilidad entre diferentes conjuntos de datos, personales y no personales. La innovación tecnológica que la genética forense está experimentando nos sugiere que el *big data* podrá marcar un punto de inflexión en la investigación criminal gracias al estudio de nuevos marcadores de ADN, como los SNP. Para maximizar sus resultados, el *big data* necesita procesar cuanta más información posible y, en su caso, reusar la información disponible. Este «reciclaje» de información supone un desafío constante a los principios de la protección de los datos personales como el principio de la limitación de la finalidad, el principio de la minimización de datos, y la limitación del plazo de conservación.

El nuevo SIE es alimentado por un mayor número de fuentes informativas que van desde los Estados miembros —ahora obligados a utilizar la plataforma SIENA para cualquier intercambio de información—, otros organismos de la Unión del ELSJ, los países terceros y las organizaciones internacionales socios, hasta las entidades privadas y los particulares. A las transmisiones de información se añade la capacidad proactiva de Europol de buscar por él solo la información mediante recursos *Open Access* o las bases de datos centralizadas o nacionales a las que se le ha otorgado acceso. Dentro de estas, destacan el SIS y el Reglamento Prüm II que permiten a Europol rastrear datos biométricos y perfiles de ADN fungiendo de puente entre los Estados miembros y terceras partes.

Las fuentes de información de Europol determinan la finalidad que Europol debe perseguir en el primer uso de los datos; el propio Europol la establece solo en el caso de que la información proceda de su búsqueda *motu proprio* o de entidades privadas y de particulares. El Reglamento Europol permite el uso ulterior de los datos personales bajo dos fórmulas principales: 1.ª Europol puede reusar la información si el proveedor lo permite, o si el tratamiento por verificación cruzada, análisis estratégico, análisis de riesgo o temático y de facilitación del intercambio de información entre Estados miembros, Europol, otros órganos de la Unión, países terceros, organizaciones internacionales y partes privadas sirve para fines de investigación científica e innovación; 2.ª los Estados miembro, organismos de la UE y los demás países terceros y organizaciones internacionales socios, en cambio, pueden acceder y reusar la información en los límites del art. 20 del mandato de Europol o en el respeto de lo pactado por el acuerdo subyacente. El episodio conocido como «el desafío de los macrodatos» resalta la problemática intrínseca de la normativa de protección de datos personales en la UE en el momento de procesar grandes conjuntos de datos complejos, eso es, en el momento de implementar la técnica del *big data*. En este sentido, la incapacidad de Europol de procesar eficazmente los datos transmitidos por los Estados miembros ha llevado la Agencia a infringir su propio Reglamento, según se desprende de las investigaciones del SEPD. En respuesta a las advertencias del SEPD, Europol ha propuesto un plan de acción para modificar el Reglamento 2016/679, centrándose en el marcado y etiquetado

[260] Art. 33 bis.4 del Reglamento Europol.

de datos, acceso restringido, revisiones periódicas y coordinación de calidad de datos. Sin embargo, las propuestas del SEPD sobre el período máximo de conservación de datos no fueron aceptadas por la Agencia que argumentaba la necesidad de mayor flexibilidad para apoyar investigaciones específicas en curso. El desafío del *big data* ha sido el catalizador para enmendar al Reglamento Europol, como se refleja en el Reglamento 2022/991, que amplía su mandato para apoyar una investigación penal. Sin embargo, el SEPD ha advertido en repetidas ocasiones que el principio de proporcionalidad no puede respetarse cuando Europol extralimita los parámetros del Anexo II de su mandato.

El régimen de tratamiento y protección de los datos genéticos ha sido introducido solo recientemente, con el Reglamento 2016/794, aunque la Agencia ha desde siempre procesado esta categoría de datos personales. Además, el Reglamento 2022/991 ha modificado este régimen, suprimiendo la prohibición de procesar las categorías especiales de datos personales previstas por el art. 30.2 en línea con la DPDP. Tal y como ha quedado reformulado, el art. 30.2 del Reglamento Europol confiere a los datos genéticos una protección reforzada que autoriza su tratamiento cuando estrictamente necesario y proporcionado para fines de proyectos de investigación e innovación y con fines operativos, sin que se puedan seleccionar grupos de personas sobre la base de estas categorías, y prohibiendo la transferencia de datos personales a terceros países u organizaciones internacionales salvo que exista otra obligación en derecho. A esto se añade que, en el caso de analizar categorías especiales de datos personales por el *big data*, el responsable del procesamiento deberá informar al responsable de la protección de datos sin demora, y realizar una EIPD en base a la naturaleza, ámbito, contexto y objetivos del tratamiento. La inclusión del concepto de perfil de ADN en la de dato genético bajo el art. 30.2 es cuestionable, pudiéndose argumentar que, en realidad, los perfiles de ADN (parte no codificante) sirven una finalidad identificadora solamente, lo que nos acercaría más al concepto de datos biométricos. Esta distinción es importante si tomamos nota de que los datos biométricos solamente pueden ser procesados autónomamente, eso es, sin necesidad de datos personales añadidos, de esta forma, es posible vincular distintos delitos aun cuando el autor se ha quedado en incógnito. En cualquier caso, al tratar perfiles de ADN (si bien la parte no codificante), Europol no puede eludir la obligación de realizar una EIPD bajo la supervisión del responsable de la protección de los datos personales. Hemos advertido que, aunque el art. 39.1 del Reglamento Europol anule la obligación de solicitar una autorización previa al SEPD respecto a un «tipo nuevo de tratamiento que implique un riesgo elevado», estas operaciones de tratamiento deben ser comunicadas al SEPD por el responsable de la protección de datos en el marco de sus obligaciones de rendición de cuentas.

Siguiendo al art. 30.2 del Reglamento Europol, el procesamiento de perfiles de ADN puede realizarse al menos en los dos supuestos siguientes: 1.ª para fines de investigación e innovación, y 2.ª para fines operativos. Hemos criticado la expresión «fines operativos» por ser demasiado amplia y no coincidir con la de «análisis operativo» del art. 18.2, let. c) del Reglamento Europol o la de «datos personales operativos» del art. 3.2 del RPDUE y hemos propuesto hacer una remisión a las (o algunas de las) tareas previstas por el art. 18.2 del Reglamento Europol. Después, nos hemos detenido en estudiar el nuevo art. 33 bis del Reglamento Europol en virtud del cual la Agencia puede procesar datos personales para proyectos de investigación e innovación en su nuevo Laboratorio. Esta disposición permitirá a la Agencia desarrollar, entrenar y validar herramientas de IA y resultará muy útil para progresar con la investigación genético-forense y, en concreto, el análisis fenotípico de ADN. Recordando que, en el contexto científico, el uso de categorías especiales de datos personales (p.e. los datos genéticos) es muy común, hemos subrayado como la base legal que legitima su tratamiento es más flexible que las demás previstas por el RGPD, si bien se necesita primero levantar la prohibición del art. 9.1 del RGPD. Nos hemos, por tanto, dedicado a resaltar las especificidades de este régimen bajo el mandato de Europol en la medida en que la Agencia quiera procesar datos personales policiales en el marco de sus proyectos. En primer lugar, se ha resaltado que el procesamiento de datos personales puede constituir un «primer uso» o un «uso ulterior» dependiendo de la clasificación que haga el proveedor de la información que proporciona los datos a Europol. A tal efecto, las autoridades competentes de los Estados miembros deberían estar empoderadas para realizar tareas no estrictamente policiales

y, de forma más específica, procesar información para fines de investigación científica por una norma con rango de ley. Cuando, en cambio, Europol usa ulteriormente la información que se había destinado previamente a tareas operativos, su Reglamento debería aclarar la obligación de notificar el proveedor para no eludir el principio de la limitación de la finalidad de conformidad con el derecho nacional de cada Estado miembro. A diferencia que el art. 89 RGPD, el art. 33 bis.2 no contempla el principio de la minimización y anonimización de datos entre las garantías reforzadas para procesar datos personales para fines de investigación científica; tampoco se enumeran los derechos subjetivos (aunque restringibles) que el titular debería poder hacer valer, si bien el deber de información a cargo del responsable del tratamiento puede restringirse para salvaguardar el interés público subyacente a los proyectos de investigación e innovación. En modo de conclusión, el art. 33 bis del Reglamento Europol prohíbe la toma de medidas o decisiones sobre los particulares a raíz de un ensayo científico, con independencia del beneficio o perjuicio que estas puedan ocasionar, lo que confirma la naturaleza meramente experimental del Laboratorio. Laboratorio que pone a disposición de la Agencia y de los Estados miembros un entorno especialmente propicio para la realización de ensayos sobre productos que aún no están preparados para la operacionalización.

Bibliografía

Alberti, Jacopo *Le agenzie dell'Unione Europea*, Giuffré Editore, Milano, 2018.

Alcalde Bezhold, Guillermo y Alfonso Farnós, Iciar «Utilización de tecnología *Big Data* en investigación clínica», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext., 2019, pp. 53-88.

Alkorta Idiakez, Itziar «Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Bigdata», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine. Genética, Biotecnología y Medicina Avanzada*, n.º ext. 1, 2019, pp. 273-323.

Barash, Mark, McNevin, Dennis, Fedorenko, Vladimir, Giverts, Pavel «Machine learning applications in forensic DNA profiling: A critical review», *Forensic Science International: Genetics*, Vol. 69, 2024, pp. 1-15.

Berthelet, Pierre «Europol face au défi de "mega-données": L'évolution tendancielle d'une coopération policière européenne "guidée par le renseignement"», *Revue du droit de l'Union Européenne*, n.º 2, 2019, pp. 157-187.

Canales Serrano, Aurora «Forensic DNA phenotyping: A promising tool to aid forensic investigation. Current situation», *Spanish Journal of Legal Medicine*, Vol. 46, n.º 4, pp. 183-190.

Carnevale, Stefania, Forlati, Serena y Giolo, Orsetta, *Redefining Organized Crime: A Challenge for the European Union*, Hart Publishing, Oxford, 2017, pp. 171-182.

Comand-Kund, Florin «Europol's International Exchanges of Data and Interoperability of AFSJ Databases», *European Public Law*, Vol. 26, n.º 1, 2020, pp. 181-204.

Coudert, Fanny «The Europol Regulation and Purpose Limitation: From the "Silo-Based Approach" to What…Exactly?», *European Data Protection Law Review*, Vol. 3, n.º 3, 2017, pp. 313-324.

de Miguel Beriain, Iñigo «El uso de datos de salud para investigación biomédica a la luz de la Propuesta de Reglamento del Parlamento Europeo del Consejo sobre el Espacio Europeo de Datos Sanitarios», *Revista jurídica de Castilla y León,* n.º 60, 2023, pp. 7-35.

de Miguel Beriain, y Mursuli Yanes, Yenifer «Sesgos, IA y biomedicina: un comentario desde la ética del Derecho», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º 59, 2023, pp. 1134-7198.

DE MONTALVO JÄÄSKELÄINEN, Federico «Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del Big Data», *UNED. Revista de Derecho Político*, n.º 106, pp. 43-75.

DE MOOR, Alexandra «The European Council Decision: Transforming Europol into an Agency of the European Union», *Common Market Law Review*, Vol. 47, n.º 4, 2010, pp. 1089-1121.

DREWER, Daniel y MILADINOVA, Vasela «The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation», *Computer Law & Security Review*, Vol. 3, n.º 33, 2017, pp. 298-308.

FERNÁNDEZ ROJO, David «La declaración de la víctima de tráfico ilegal de migrantes como prueba preconstituida y las corroboraciones externas que han de reforzar su verosimilitud», *Revista de Derecho Comunitario Europeo*, n.º 123, pp. 65-98.

GABRIELLE, Samuel y PRAINSACK, Barbara *The regulatory landscape of forensic DNA phenotyping in Europe VISAGE*, King's College London, Londres, 2018.

GARCÍA, Oscar y ALONSO, Antonio «Las bases de datos de perfiles de ADN como instrumento en la investigación policial» ROMEO CASABONA, Carlos María (Ed) *Bases de datos de perfiles de ADN y criminalidad*, Comares, Granada, 2002, pp. 27-44.

GOIZUETA VÉRTIZ, Juana «La cooperación policial en el seno de Europol: el principio de disponibilidad y la confidencialidad de la información», *Revista Española de Derecho Constitucional*, n.º 110, pp. 75-103.

HOEK, Dante y STIGTER, Jill «Europol: an overwhelming stream of Big Data», *Revue Internationale De Droit Pénal*, Vol. 2, n.º 92, 2021, pp. 19-44.

JASSERAND, Catherine «Processing of special categories of personal data» KOSTA, Eleni y BOHEM, Franziska (Eds) *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, pp. 217-230.

JOHNSON, Paul y WILLIAMS, Robin «Internationalizing New Technologies of Crime Control: Forensic DNA Databasing and Datasharing in the European Union», *Policing & Society*, Vol. 2, n.º 17, 2007, pp. 103-118.

KURU, Taner «C-205/21 *VS v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnoost*: Indiscriminate and Generalised Collection of Biometric and Genetic Data by law Enforcement Authorities in the EU Is Not Allowed», *European Data Protection Law*, Vol. 10, n.º 2, 2024, pp. 223-231.

KUSAK, Martyna «Quality of data sets that feed AI and big data applications for law enforcement», *ERA Forum*, n.º 23, 2022, pp. 209-219.

LAI, Wanqi, VAN VARENBERGH, Amalia, y BELLAERT, Wannes «Europol and its growing Alliance with private parties», *Revue Internationale de Droit Pénal*, Vol. 92, n.º 2, 2021, pp. 45-66.

LAZCOZ MORATINOS, Guillermo *Gobernanza y supervisión humana de la toma de decisiones automatizada basada en la elaboración de perfiles,* Universidad del País Vasco (UPV/EHU), 2023.

LEGIND LARSEN, Henrik, BLANCO, José María, PASTOR PASTOR, Raquel, y R. YAGER, Ronald *Using Open Data to Detect Organized Crime Threat: Factors Driving Future Crime*, Springer, Berlín, 2017.

LIÑÁN NOGUERAS, Diego Javier «El sistema jurisdiccional de la Unión Europea» MANGAS MARTÍN, Araceli y LIÑÁN NOGUERAS, Diego Javier (Eds) *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, pp. 473-506, p. 481.

LORENTE ACOSTA, José Antonio «Identificación genética criminal: importancia médico legal de las bases de datos de ADN» ROMEO CASABONA, Carlos María (Ed) *Bases de datos de perfiles de ADN y criminalidad*, Comares, Granada, 2002, pp. 1-26

LORENTE, José A., SAIZ, María, HAARKÖTTER, Christian, ROBLES-FERNÁNDEZ, Inmaculada, ÁLVAREZ-CUBERO, J. María, GÁLVEZ, Xiomara, MARTÍNEZ-GONZÁLEZ, Luis J., LORENTE-REMÓN, Begoña, ÁLVAREZ, Juan C. «Genetic identification against traffic in human beings», *Forensic Science*, 2020, pp. 1-13.

MALANDA, Sergio y ROMEO CASABONA, Carlos María *La identificación del ADN en el Sistema de Justicia Penal*, Thomson Reuters Aranzadi, Pamplona, 2010.

MARICA, Andrea *El sistema de tratamiento de la información de EUROPOL,* Working Paper n.º 309, Instituto de Ciencias Políticas y Sociales de la Universidad Autónoma de Barcelona, Barcelona, 2012.

MARRERO ROCHA, Inmaculada «Nuevas dinámicas en las relaciones entre crimen organizado y grupos terroristas», *Revista española de derecho internacional*, Vol. 69, n.º 2, 2017, pp. 145-169.

MARTANI, Andrea, DARRYL GENEVIÈVE, Lester, PAULI-MAGNUS, Christiane, MCLENNAN, Stuart, y SIMONE ELGER, Bernice «Regulating the Secondary Use of Data for Research: Arguments Against Genetic Exceptionalism», *Frontiers in Genetics*, Vol. 10, n.º 1254, 2019, pp. 1-11.

MERINO GÓMEZ, Gustavo «Nuevos desafíos en torno al big data», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext. 1, 2019, pp. 37-54.

MÉSZÁROS, János y HO, Chih-hsing, «The Big Data and Scientific Research: The Secondary Use of Personal Data under Research Exemption in the GDPR», *Hungarian Journal of Legal Studies*, Vol. 59, n.º 4, 2018, pp. 403-419.

MIÑO VÁSQUEZ, Verónica Gabriela «La protección de datos genéticos en virtud del Reglamento General de Protección de Datos», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º 51, 2019, pp. 77-90.

MORENTE PARRA, Vanessa «Big Data o el arte de realizar datos masivos. Una reflexión crítica desde los derechos fundamentales», *Derechos y libertades*, Vol. 2, n.º 4, 2019, pp. 225-260.

NEIVA, Laura «Big Data technologies in criminal investigations: The frames of the members of Judiciary Police in Portugal», *Criminology & Criminal Justice*, Vol. 0, n.º 0, 2023, pp. 1-23.

NEIVA, Laura, GRANJA, Rafaela, y MACHADO, Helena «Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union», *Policing and Society*, Vol. 10, n.º 32, pp. 1167-1179.

NICOLÁS JIMÉNEZ, Pilar «Ficheros policiales de perfiles ADN (Comentario al art. 22 LOPD)» TRONCOSO REIGADA, Antonio (Ed) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Thomson Reuters Aranzadi, Pamplona, 2010, pp. 1428-1456.

NICOLÁS JIMÉNEZ, Pilar «Investigación con muestras biológicas y biobancos» ROMEO CASABONA, Carlos María, *Manual de bioderecho*, Dykinson, Madrid, 2022.

NICOLÁS JIMÉNEZ, Pilar *La protección jurídica de los datos genéticos de carácter personal*, Comares, Granada, 2006.

NICOLÁS JIMÉNEZ, Pilar «Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext., 2019, pp. 129-167.

PI LLORENS, Montserrat «El nuevo mapa de las agencias europeas del espacio de libertad, seguridad y justicia», *Revista de Derecho Comunitario Europeo*, n.º 56, 2017, pp. 77-117.

QUINTEL, Teresa «The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation: The Question of Legitimizing Unlawful Practices», *European Data Protection Law Review*, Vol. 1, n.º 8, 2022, pp. 90-102.

RECUERO LINARES, Mikel «El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales», *InDret*, n.º 2, 2024, pp. 525-551.

RECUERO LINARES, Mikel *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectivas europea ante el desafío globalizado*, AEPD, Madrid, 2019, n.º 9.

ROMEO CASABONA, Carlos María «Datos biométricos (Comentario al artículo 4.14 RGPD)» TRONCOSO REIGADA, Antonio (Ed) *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo I, Thomson Reuters Aranzadi, Pamplona, pp. 709-714.

ROMEO CASABONA, Carlos María «Revisión de las categorías jurídicas de la normativa europea ante la tecnología del *big data* aplicada a la salud», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º ext. 1, 2019, pp. 85-127.

ROSANÓ, Alessandro «Protecting Europe beyond its Borders: The Agreements between Europol and Third States or International Organizations», *Cadernos de Dereito Actual*, n.º 4, 2016, pp. 9-21.

SÁNCHEZ RUBIO, Ana «Reflexiones sobre la todavía polémica prueba de ADN: análisis de tres posibles escenarios de su inadmisión probatoria», *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada/Law and the Human Genome Review. Genetics, Biotechnology and Advanced Medicine*, n.º 52, 2020, pp. 169-193.

SANTOS VARA, Juan «Las consecuencias de la integración de Europol en el Derecho de la Unión Europea: comentario a la Decisión del Consejo 2009/371/JAI, de 6 de abril de 2009», *Revista General de Derecho Europeo*, n.º 20, 2010, pp. 2-24.

SATPATHY, Suneeta y MOHANTY, Sachi *Big Data Analytics and Computing for Digital Forensic Investigations*, CRC Press, BocaRaton/Oxon, 2020.

SHEN, Hong y MA, Jian «Privacy Challenges of Genomic Big Data» R. COHEN, Irun, LAJTHA, Abel, D. LAMBRIS, John, y PAOLETTI, Rodolfo (Eds) *Advances in Experimental Medicine and Biology*, Springer, Berlín, 2017, pp. 139-148.

TAS, Sarah «The dangerous increasing support of Europol in national criminal investigations: An additional layer of complexity», *New Journal of European Criminal Law*, Vol. 4, n.º 14, 2023, pp. 534-551.

TASSINARI, Francesca *Data Protection and Interoperability in EU External Relations: Guaranteeing global data transfers in the area of freedom, security and justice*, Brill/Nijhoff, Leiden, 2024, en prensa.

TASSINARI, Francesca «Issues of consistency and complementarity in EU privacy law: The Europol's Big Data challenge», *Revista General de Derecho Europeo,* n.º 63, 2024, pp. 133-169.

TOOM, Victor *Cross-Border Exchange and Comparison for Forensic DNA Data in the Context of the Prüm Decision*, Estudio para la Comisión LIBE, Bruselas, 2018.

VALLS PRIETO, Javier *Problemas jurídicos penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*, Dykinson Madrid.

VAVOULA, Niovi «Surveillance of Foreign Terrorism Fighters via the Schengen Information System (SIS): Towards Maximum Operationalisation of Alerts and an Enhanced Role for Europol», *New Journal of European Criminal Law*, 2023, Vol. 2, n.º 14, pp. 206-230.

VAVOULA, Niovi, *Immigration and Privacy in the Law of the European Union. The Case of Information Systems*, Brill/Nijhoff, Leiden, 2022.

VLADIMIROVNA BOGDAN, Varvara y ANATOLYEVNA KIRILLOVA, Elena «Problems of personal data protection when using big data technologies», *Journal of applied engineering science,* Vol. 3, n.º 18, pp. 438-442.

VOGIATZOGLOU, Plixavra y MARQUENIE, Thomas *Assessment of the implementation of the Law Enforcement Directive*, Estudio para la Comisión LIBE, Bruselas, 2022.

WESTERMARK, Henrik, ARONOVITZ, Alberto, CURRAN, John, FAUSCH, Inesa, FOURNIER, Johanna, HOHENECKER, Lukas, KLECZEWSKI, Anne-Grace PRETELLI, Ilaria, POLANCO LAZO, Rodrigo, TOPAZ DRUCKMAN, Karen, VIENNET, Carole, WENT, Floriaan, ZHENG, Jun *The Regulation of the Use of DNA in Law Enforcement*, Instituto suizo de derecho comparado, Lausanne, 2020.