Integración Regional & Derechos Humanos / Revista Regional Integration & Human Rights / Review

Año XII – Nº 2 – 2º semestre 2024

Centro de Estudios Integración Regional & Derechos Humanos

IR & DH

Facultad de Derecho Universidad de Buenos Aires

FACULTAD DE DERECHO · UNIVERSIDAD DE BUENOS AIRES ·

Integración Regional & Derechos Humanos /Revista Regional Integration & Human Rights /Review

Revista del Centro de Estudios
Integración Regional & Derechos Humanos
Facultad de Derecho
Universidad de Buenos Aires – Argentina

Año XII – N°2 – Segundo semestre 2024

ISSN: 2346-9196

Av. Figueroa Alcorta 2263 (C1425CKB)
Buenos Aires - Argentina
revistairydh@derecho.uba.ar

¿CUÁNDO EL FIN JUSTIFICA LOS MEDIOS? INTELIGENCIA ARTIFICIAL (IA) Y DATOS BIOMÉTRICOS EN PASAPORTES Y DOCUMENTOS DE IDENTIDAD. JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Calogero Pizzolo [1]

Resumen

Este escrito aborda el desarrollo de la biometría de primera generación –en relación con la recolección de huellas dactilares e imágenes faciales- para la identificación de personas. El almacenamiento de estos datos biométricos, en dispositivos de pasaportes y documentos de identidad, es abordado directamente por la jurisprudencia de los jueces con sede en Luxemburgo. La limitación al derecho a la intimidad y al derecho a la protección de datos de carácter personal queda acreditada, y la jurisprudencia avanza entonces en la interpretación de los requisitos para que dicha limitación sea legítima. Finalmente, el autor deja en evidencia la inestable frontera entre verificación e identificación de personas a partir de datos biométricos y la posible intervención de la IA en estas operaciones. Intervención que, en muchos casos, terminará siendo determinante para establecer la legalidad de la restricción a los derechos.

Palabras clave: Inteligencia Artificial (IA) – Datos biométricos – Pasaportes y documentos de identidad – Derecho a la Intimidad – Derecho a la protección de datos de carácter personal – Unión Europea

Title: WHEN DOES THE END JUSTIFY THE MEANS? ARTIFICIAL INTELLIGENCE (AI) AND BIOMETRIC DATA IN PASSPORTS AND IDENTITY DOCUMENTS. JURISPRUDENCE OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

Abstract:

[1] Profesor titular ordinario de Derecho de la Integración y de Derechos Humanos y Garantías, ambas asignaturas en la Facultad de Derecho de la Universidad de Buenos Aires. Catedrático Jean Monnet en Derecho Público Europeo. Director del Centro de Estudios sobre “Integración Regional & Derechos Humanos”.

This article addresses the development of first-generation biometrics – in relation to the collection of fingerprints and facial images – for the identification of persons. the storage of these biometric data, in passport and identity document devices, is directly addressed by the case law of the judges based in Luxembourg. the limitation to the right to privacy and the right to the protection of personal data is proven, and the case law then advances in the interpretation of the requirements for such limitation to be legitimate. finally, the author highlights the unstable border between verification and identification of persons from biometric data and the possible intervention of ai in these operations. intervention that, in many cases, will end up being decisive in establishing the legality of the restriction on rights.

Keywords: Artificial Intelligence (AI) – Biometric data – Passports and identity documents – Right to Privacy – Right to the protection of personal data – European Union.

I. IA y Biometría: alcances y contenidos en datos personales

¿Cuándo el fin justifica los medios? En la respuesta a esta pregunta -tan superficial como profunda- creemos radica la esencia de la relación, presente y futura, entre el ser humano y la IA. En el caso que hoy nos ocupa, ¿hasta qué punto estamos dispuesto a resignar espacios de libertad individual -autodeterminación informativa-, para verificar o identificar a las personas, con el fin de garantizarnos una mayor seguridad o una información más confiable sobre quiénes somos? ¿Cuál es el límite, la frontera que no estamos dispuesto a cruzar? ¿Cuál es la nueva dimensión que estamos dispuestos a reconocerle al Estado de Derecho en la forzada transición hacia una sociedad digital, hacia a una realidad híbrida?

Se ha puesto de manifiesto que la IA no crea problemas por sí misma, son los hombres que la diseñan y la utilizan los que generan los riesgos para los valores de convivencia básicos. Estamos hablando de sistemas de información sobre los que se ejecutan procesos informáticos (algorítmicos) de aprendizaje y/o de decisión. Ello requiere: datos adecuados, reglas y procesos de

aprendizaje, y propuestas de decisión (*outputs*) sometidas o no a supervisión y validación humana. No se trata, pues, de entes autónomos dotados de razón. Es una máquina de diseño humano, controlada por humanos y al servicio de los humanos (BUSTOS GISBERT: 2024, p. 155).

Aunque no existe una definición técnica unánimemente compartida de IA, podemos coincidir con la doctrina en un elemento descriptivo (a-técnico), útil para enmarcar el tema: la IA crea, por así decirlo, un mundo nuevo, *híbrido* porque es virtual y, al mismo tiempo, (absolutamente) real por su impacto en las personas, los derechos y las libertades. En particular, la IA afecta al desarrollo de la persona, fragmenta la identidad personal e interactúa, habla con los usuarios y, al hacerlo, desafía al ser humano, el único ser dotado de palabra. A medida que la IA se perfecciona, las preguntas se amplían y no se refieren sólo a la naturaleza y los límites que se deben imponer a la IA, sino que terminan incluyendo la propia condición humana (DE SANTIS: 2024, p. 138). La realidad física y la digital representan ámbitos que tienen unas condiciones estructurales propias cada una de ellas. La realidad física no es igual que la digital y ambas confluyen en un mundo híbrido que las integra a las dos. La *realidad híbrida* está cada vez más presente en nuestras sociedades y en nuestros sistemas jurídicos. La realidad digital se ha ido ampliando, comprimiendo la realidad física o proyectándose progresivamente sobre esa realidad física. Nuevas pautas culturales y nuevos paradigmas se están desarrollando en un proceso de digitalización de la vida que parece no tener fin (BALAGUER CALLEJÓN: 2023, p. 42).

Podría argumentarse que, los datos biométricos, representan una *forma de digitalización del cuerpo humano*. Éste, o más bien cada una de sus partes, se convierten directamente en fuentes de información digital a través de las cuales es posible identificar a personas individuales. El rostro de una persona, o bien sus huellas dactilares, el ADN, la forma del iris, la voz, pero también el comportamiento; son como una especie de códigos de barras que emiten señales con las que se distingue a los individuos entre sí. Esta identificación es posible porque los datos biométricos obtenidos de este modo comparten algunas características esenciales: a) *universalidad*, todas las personas tienen los mismos elementos físicos; b) *distinguibilidad*, estos datos se basan en

características biométricas únicas; c) *permanencia*, estas características permanecen casi inalteradas a lo largo de la vida de una persona; y d) *recopilabilidad*, la información recopilada de esta manera puede almacenarse, utilizarse y reutilizarse.

Establecer una definición legal inequívoca de los datos biométricos es, a la vez, algo problemático, ya que el progreso científico y los avances tecnológicos amplían constantemente la posibilidad de adquirir y procesar este tipo de datos, lo que impide proporcionar un marco estático y definitivo (MOBILO: 2021, pp. 136-137).

1. Reglamento (UE) 2024/1689: dato biométrico e IA

El flamante Reglamento (UE) 2024/1689[2] sobre IA define a los *datos biométricos* como "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos" (artículo 3, apartado 34).[3]

Mientras que por *identificación biométrica* entiende "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos" (artículo 3, apartado 35). Esta técnica permite identificar al sujeto sin necesidad de interacción física con el interesado. Las mediciones realizadas con una videocámara o un micrófono son adquiridas por IA y procesadas comparando las características biométricas con los datos previamente adquiridos y almacenados en una base de datos y/o diferentes bases de datos.

La *verificación biométrica*, por su parte, es definida como "la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las

[2] 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) nº 300/2008, (UE) nº 167/2013, (UE) nº 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 (Texto pertinente a efectos del EEE).

[3] Este concepto de datos biométricos -afirma el propio Reglamento (UE) 2024/1689 en su considerando 14- "debe interpretarse a la luz del concepto de «datos biométricos» tal como se define en el artículo 4, punto 14, del Reglamento (UE) 2016/679, en el artículo 3, punto 18, del Reglamento (UE) 2018/1725, y en el artículo 3, punto 13, de la Directiva (UE) 2016/680".

personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente" (artículo 3, apartado 36).

Los *sistemas biométricos de reconocimiento* utilizan un dato y lo comparan con una lista o base de datos, como sucede con las bases de datos criminales, mientras que los *sistemas biométricos de verificación* sólo utilizan un dato comparándolo con el mismo dato previamente almacenado, como es el caso de las bases migratorias. Cada vez más se emplean sistemas biométricos de reconocimiento o autenticación con dos o más datos biométricos, que se denominan "sistemas de combinación biométrica", en los que pueden valorarse el peso, la altura, el tipo de sangre, factor sanguíneo, entre otros.

2. Elementos para una conceptualización del dato biométrico

La definición legal de dato biométrico incluye, según notamos, tanto propiedades físicas o fisiológicas (huellas digitales, voz, forma de las orejas o el rostro, parámetros de la retina o del iris, etc.), como psicológicas o comportamentales (tics, análisis de pulsaciones de teclas, la firma manuscrita o la forma de caminar, entre otros) siempre que permitan la identificación unívoca de una persona.

Para calificar, por lo tanto, a un dato personal de biométrico los *criterios* que se siguen son tres: a) su *naturaleza*, esto es, las características físicas, fisiológicas o conductuales de un individuo; b) los *medios y las formas de tratamiento*, han de obtenerse a partir de un tratamiento técnico específico; y c) la *finalidad* del tratamiento: la identificación unívoca de una persona física.

Los datos biométricos -lo cual se manifiesta como uno de sus rasgos esenciales-, cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que permiten que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior. Lo dicho, hace que los sistemas biométricos sean capaces de identificar unívocamente a una persona utilizando determinadas cualidades fisiológicas o comportamentales únicas. Condición que los convierte en mucho más fiables que otros tipos de datos personales, pero, al mismo tiempo, su utilización inadecuada supondrá mayores peligros para los Derechos.

Se llega a distinguir entre *identificadores fuertes* especialmente utilizados con las tecnologías de primera generación destinadas a la identificación, e *identificadores débiles* que cada vez cobran más protagonismo (formas de andar, patrones de vasos sanguíneos, pulsaciones de teclas etc.). Con la nueva generación de tecnologías se va más allá de la finalidad de identificación y se habla de "biometría del comportamiento" para el perfilado, reconocimiento de emociones o categorización de personas. Es por ello que, frente a los datos biométricos ligados únicamente a la identificación, se propone el concepto más amplio inclusivo de "datos basados en la biometría" (COTINO HUESO: 2023, p. 353).

En la actualidad la biometría se vincula a los sistemas automatizados de *identificación,* entendida como el proceso de reconocimiento de un individuo particular entre un grupo, y *autenticación,* el proceso de probar que es cierta la identidad reclamada por el individuo. Estos sistemas pueden servir para identificar colectividades, en atención a rasgos identitarios de grupos, o referirse tan solo a datos biométricos de personas individualmente consideradas, siendo esta última la que ha impulsado especialmente los desarrollos biométricos informáticos, desde los que se trabaja con los datos almacenados en soporte informático para ofrecer respuestas de reconocimiento e identificación individual (BARONA VILAR: 2024, p. 302).

La biometría, en sí, incluye el conjunto de tecnologías que permiten la captura o registro de algún rasgo del cuerpo humano, la conversión en información digital de ese registro y su almacenamiento en grandes bancos de datos que podrán estar disponibles para autentificación, identificación y verificación por parte de Estados o empresas. Abarcaría todos los procesos automatizados que se utilizan para identificar a un individuo mediante patrones físicos, fisiológicos o comportamentales y, estas características, se definen como datos biométricos, ya que permiten o confirman la identificación única de una persona.

Estas tecnologías han ido evolucionando. Comenzamos hablando de la *biometría fisiológica* o de primera generación que registra características físicas que permiten individualizar al sujeto como las huellas digitales, la estructura venosa, geometría o impresión de la palma de la mano, el reconocimiento facial,

de iris o de retina, o el ADN, entre otros para establecer la identidad de una persona permitiendo su verificación y autenticación. Para llegar hasta la *biometría conductual*. Esta biometría de segunda generación o de medición de la conducta analiza características relacionadas con el patrón de comportamiento con el objetivo de predecir conductas sospechosas o intenciones hostiles y uno de sus objetivos es establecer perfiles de personas con base en la predicción de sus acciones y conductas mediante cámaras capaces de reconocer esos rasgos.

Como observamos, la definición de biometría se ha ampliado para incluir características invisibles de una persona, como el comportamiento y las emociones, la dinámica facial, los estados psicológicos, los niveles de excitación (miedo, ansiedad, intención) y las células, fluidos o rastros corporales (como el ADN o las imágenes cerebrales en medicina forense), con el análisis de los gestos anticipatorios, la paralingüística y las imágenes térmicas.

El Supervisor Europeo de Protección de Datos advertía, ya hace algunos años, que nunca carece de importancia la elección del uso de la biometría en sistemas de información, especialmente cuando el sistema en cuestión afecta a un número tan grande de personas. Aunque el ojo humano no pueda leer las características biométricas, sí pueden hacerlo, y hacer uso de ellas, los instrumentos adecuados, sin límite de tiempo y dondequiera que la persona se encuentre.[4]

A continuación, analizamos la jurisprudencia del Tribunal de Justicia en relación con la recogida y almacenamiento de las impresiones dactilares en pasaportes y documentos de identidad. Es importante tener presente, en el análisis que sigue, que lo que se interpreta en Luxemburgo es la legalidad de un tratamiento de datos personales con la finalidad explícita de *verificar* la identidad de la persona titular del documento en cuestión. Es decir, no se trata de justificar apelar a la biometría para crear bases de datos generales que permitan a los algoritmos -y a través de ellos a la IA- identificar a personas, ni mucho menos

[4] Dictamen de 23 de marzo de 2005 sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de información de visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (DO C 181, p. 13). Citado en las Conclusiones del Abogado General Paolo Mengozzi presentadas el 13 de junio de 2013, asunto C 291/12 [ECLI:EU:C:2013:401], *Schwarz*, apartado 1.

crear categorías de personas. Delinear esta frontera, muchas veces difusa, entre *verificar* "uno-a-uno" e *identificar* "uno-a-varios", puede constituir la diferencia entre la validez o invalidez jurídica de la legislación en la materia aplicada a un caso en cuestión.

II. Afectación directa al derecho a la intimidad: los artículos 7 y 8 de la Carta de Derechos Fundamentales de la UE (CDFUE)

Las técnicas biométricas, influyen sobre el proceso de identificación poniendo en riesgo la protección de la libertad personal y la privacidad (DE SANTIS: 2024, p. 156; MOLLO: 2024, p. 111). En la misma línea ya se había expresado el Grupo de Trabajo previsto en el artículo 29 (de la entonces Directiva 95/46/CE[5]). Debido a los riesgos específicos aparejados a la utilización de datos biométricos, se recomiendó que quien defina la finalidad y los medios del dispositivo realice evaluaciones del impacto en la intimidad como parte integrante de la fase de diseño de los sistemas que tratan este tipo de datos. Dichas evaluaciones, entre otras, deberían tener en cuenta la naturaleza y la finalidad de la información recogida, medidas menos invasivas de la intimidad a las previstas, y las decisiones tomadas en cuanto al tiempo de conservación y la supresión de los datos. Las evaluaciones del impacto en la intimidad no solo deberían orientarse a la identificación de los riesgos, también deberían proporcionar medidas adecuadas de protección de datos.[6]

Las medidas legislativas -explica la EDPB, *European Data Protection Board*- que sirven de base jurídica para el tratamiento de datos personales "interfieren directamente" en los derechos garantizados por los artículos 7 y 8 (CDFUE). El tratamiento de datos biométricos "*constituye en sí mismo una grave injerencia en cualquier circunstancia y con independencia del resultado*".[7] El tratamiento de categorías especiales de datos, como los datos biométricos, solo

[5] Como sabemos derogado por el 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.
[6] Grupo de Trabajo del artículo 29, Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012, p. 32.
[7] EDPB, "Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley" (Versión 2.0). Adoptada el 26 de abril de 2023, p. 5 (también apartados 36 y 38). Sin resaltar en el original.

puede considerarse “estrictamente necesario” si la injerencia en la protección de los datos personales y sus restricciones se limitan a lo absolutamente necesario, es decir, indispensable, y “excluyen todo tratamiento de carácter general o sistemático”.[8]

La CDFUE -instrumento de última generación en la tutela regional de derechos-, en su artículo 7 prescribe que toda persona tiene derecho al respeto de su vida privada y familiar[9]. Mientras que, en su artículo 8, apartado 1, sostiene que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.[10] Interpretadas -afirma el Tribunal de Justicia-, “*conjuntamente, de estas disposiciones se infiere que, en principio, puede constituir una vulneración de tales derechos cualquier tratamiento de datos personales por parte de un tercero*”.[11]

En el asunto *Digital Rights Ireland* (2014)[12] en Luxemburgo ya habían detectado que, un tratamiento de datos de carácter personal, podría significar “una injerencia” en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 (CDFUE)”. Siguiendo al Abogado General Cruz Villalón, el Tribunal de Justicia califica el alcance de dicha injerencia -atribuida a la Directiva 2006/24[13]- en los derechos fundamentales reconocidos

[8] *Ídem*, p. 6.
[9] La norma citada dice: “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”.
[10] La norma citada dice: “1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.”
[11] STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartado 25. Sin resaltar en el original.
[12] STJ de 8 de abril de 2014, *Digital Rights Ireland y otros,* asuntos acumulados C 293/12 y C 594/12, [ECLI:EU:C:2014:238].
[13] En este asunto se anuló la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre conservación de datos de tráfico y localización de comunicaciones electrónicas que perseguía garantizar la disponibilidad de esos datos con fines de prevención, investigación, detección y enjuiciamiento de delitos graves -la delincuencia organizada y el terrorismo- y, a tal fin, obligaba a las compañías proveedoras de estos servicios a conservar los datos de tráfico y de localización y los necesarios para identificar al abonado o al usuario pero no amparaba, sin embargo, la conservación del contenido de las comunicaciones. Estos datos, considerados en su conjunto, según el Tribunal de Justicia podían proporcionar indicaciones muy precisas sobre la vida privada de las personas cuyos datos se conservasen, como los hábitos de la vida cotidiana, los lugares de residencia permanente o temporal, los desplazamientos diarios u otros, las actividades realizadas, las relaciones sociales y los medios sociales frecuentados. Por ello, se concluyó que la Directiva se inmiscuía de manera especialmente grave en los

en los artículos 7 y 8 (CDFUE), como de "*gran magnitud y debe considerarse especialmente grave*. Además, la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante".[14] La protección de los datos de carácter personal, consiguientemente "tiene una importancia especial para el derecho al respeto de la vida privada consagrado en el artículo 7 (CDFUE)".[15]

Para los jueces de Luxemburgo, el respeto del derecho a la vida privada, en lo que atañe al tratamiento de los datos de carácter personal, "se aplica a toda información sobre una persona física identificada o identificable".[16] Las *impresiones dactilares* "están comprendidas en este concepto por contener objetivamente información única sobre personas físicas y permitir su identificación precisa".[17]

La recopilación, procesamiento y análisis de grandes cantidades de datos personales para alimentar algoritmos de IA plantea serios desafíos para la protección de la privacidad y el derecho a la autodeterminación informativa. Por eso es necesario establecer límites claros en cuanto al uso de datos personales y asegurar que se cumpla con los principios de proporcionalidad y necesidad en la recopilación y procesamiento de los mismos (CASTELLANOS CLARAMUNT: 2023, pp. 279-280).

El debate sobre la legalidad de la recogida y almacenamiento de las impresiones dactilares llega al Tribunal de Justicia frente a las dudas que se generan en relación con los citados artículos 7 y 8 (CDFUE). En particular, el

derechos fundamentales al respeto a la privacidad y a la protección de datos de carácter personal y podía generar en las personas afectadas el sentimiento de que su vida privada era objeto de una vigilancia constante.

[14] STJ de 8 de abril de 2014, *Digital Rights Ireland y otros,* asuntos acumulados C 293/12 y C 594/12, [ECLI:EU:C:2014:238], apartados 36-37. Sin resaltar en el orginal.

[15] *Ídem*, apartado 53.

[16] STJ de 9 de noviembre de 2010, *Volker und Markus Schecke y Eifert*, asuntos acumulados C 92/09 y C 93/09 [ECLI:EU:C:2010:662], apartado 52; STJ de 24 de noviembre de 2011, *ASNEF y FECEMD*, asuntos acumulados C 468/10 y C 469/10 [ECLI:EU:C:2011:777], apartado 42; y STJ de 3 de octubre de 2019*, A y otros*, asunto C 70/18 [ECLI:EU:C:2019:823], apartado 54.

[17] Cfr. STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartado 27, donde se sigue la STEDH de 4 de diciembre de 2008, *S. y Marper c. Reino Unido* [Demandas nº 30562/2004 y 30566/2004], apartados 68 y 84.

escrutinio de los jueces de Luxemburgo alcanza al Reglamento nº 2252/2004[18] y al Reglamento 2019/1157[19]. El primero en el asunto *Schwarz* (2013)[20], el segundo en el asunto *R. L.* (2024)[21]. En ambos, se mantuvo que los derechos reconocidos por los artículos 7 y 8 (CDFUE) para el Tribunal de Justicia "*no constituyen prerrogativas absolutas, sino que deben ser considerados en relación con su función en la sociedad"*.[22]

El Reglamento nº 2252/2004 (artículo 1, apartado 2) sostiene que los *pasaportes y documentos de viaje*[23] "incluirán un soporte de almacenamiento que contendrá una imagen facial. Los Estados miembros también incluirán impresiones dactilares en modelos interoperables. Los datos deberán estar protegidos y el soporte de almacenamiento deberá tener la suficiente capacidad y la posibilidad de garantizar la integridad, la autenticidad y la confidencialidad de los datos". En este caso, el Tribunal de Justicia interpretó que la toma y

[18] Reglamento (CE) n° 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros (*DO L 385 de 29.12.2004, p. 1–6*).

[19] Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación (DO L 188 de 12.7.2019, p. 67/78).

[20] Se trata de una petición de decisión prejudicial presentada en el en el marco de un litigio entre el Sr. Schwarz y la *Stadt Bochum* (ciudad de Bochum, Alemania) en relación con la negativa de ésta a expedirle un pasaporte sin tomar simultáneamente sus impresiones dactilares para ser almacenadas en el pasaporte.

[21] La petición de decisión prejudicial se presenta en el contexto de un litigio entre R. L y el *Landeshauptstadt Wiesbaden* (Ayuntamiento de Wiesbaden, capital del estado federado de Hesse, Alemania) en relación con la denegación por este último de su solicitud de expedición de un documento de identidad que no incluya sus impresiones dactilares. Desde el 2 de agosto de 2021, la integración de dos impresiones dactilares en el medio de almacenamiento de los documentos de identidad es obligatoria en virtud del artículo 5, apartado 9, de la PAuswG, que transpone al orden jurídico alemán el artículo 3, apartado 5, del Reglamento 2019/1157.
El Tribunal de Justicia va a anular el Reglamento 2019/1157 porque entiende fue adoptado sobre una base jurídica incorrecta, manteniendo sus efectos en vigor hasta que se dicte un acto sustitutivo según las reglas de competencia. Pero va a rechazar las otras dos imputaciones planteadas por el juez alemán afirmando que la recogida de huellas dactilares y su almacenamiento en un soporte de almacenamiento en el documento no viola la CDFUE, y las Instituciones de la UE no estaban obligadas a realizar una evaluación del impacto de dichas medidas sobre la protección de datos.

[22] Entre otras, STJ de 9 de noviembre de 2010, *Volker und Markus Schecke y Eifert*, asuntos acumulados C 92/09 y C 93/09 [ECLI:EU:C:2010:662], apartado 48; STJ de 5 de mayo de 2011, *Deutsche Telekom*, asunto C 543/09 [ECLI:EU:C:2011:279], apartado 51; STJ 20 de septiembre de 2022, *SpaceNet y Telekom Deutschland*, asuntos acumulados C 793/19 y C 794/19, [ECLI:EU:C:2022:702], apartado 63; y STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 75. Sin resaltar en el original.

[23] Después de los ataques del 11 de septiembre de 2001, Estados Unidos introdujo pasaportes biométricos y exigió que cualquiera que ingresara al país tuviera uno. El legislador de la Unión siguió el mismo camino, para permitir el acceso de los ciudadanos de la Unión a Estados Unidos.

conservación de impresiones dactilares, "constituyen una vulneración" de los derechos al respeto de la vida privada y a la protección de los datos de carácter personal. Por consiguiente, ha de examinarse si tal vulneración "resulta justificada".[24] En el mismo sentido, se manifestó el Abogado General Mengozzi para quien, salvo que se renuncie a poseer un pasaporte y, por consiguiente, a desplazarse a la mayor parte de terceros Estados, los solicitantes no pueden oponerse a la recogida y almacenamiento de sus impresiones dactilares. Consiguientemente se genera "una lesión" del derecho reconocido en el artículo 8 (CDFUE).[25]

El Reglamento 2019/1157 (artículo 3, apartado 5), por su parte, afirma que los *documentos de identidad*[26]*,* "incluirán un medio de almacenamiento de alta seguridad que contendrá una imagen facial del titular del documento y dos impresiones dactilares en formatos digitales interoperables". También en este caso el Tribunal de Justicia entiende que se produce "una limitación tanto del derecho al respeto de la vida privada como del derecho a la protección de los datos de carácter personal".[27]

III. El reconocimiento de las impresiones dactilares en los sistemas biométricos: algunas consideraciones

El reconocimiento de las impresiones dactilares es uno de los sistemas biométricos más antiguos, lleva utilizándose más de 100 años con fines policiales para la *identificación* y *verificación*. Se basa, en el hecho de que cada individuo tiene impresiones dactilares únicas que muestran características específicas que pueden medirse para decidir si una impresión dactilar

[24] STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartados 29 y 30.
[25] Conclusiones del Abogado General Paolo Mengozzi presentadas el 13 de junio de 2013, asunto C 291/12 [ECLI:EU:C:2013:401], *Schwarz*, apartado 42.
[26] En el DUE, los datos biométricos se incluyen en -además de los documentos de viaje y de identidad (pasaportes y documentos de identidad)- en otros documentos (permisos de residencia, tarjetas de residencia, tarjetas de residencia permanente, certificados de residencia). También es necesario mencionar el modelo uniforme de visado digital, establecido por el Reglamento 1683/95, que contiene únicamente datos biométricos consistentes en la imagen del rostro.
[27] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 73.

corresponde con una muestra registrada. Este registro exige que la persona esté físicamente presente.

Los sistemas más avanzados son los denominados sistemas automáticos de identificación dactilar (SAID), utilizados con fines policiales y que pueden usarse para el intercambio de datos, buscando en diferentes depósitos en emplazamientos transfronterizos. En estos casos, su utilización en bases de datos a gran escala, impone la necesidad de garantizar la proporcionalidad.

El uso de impresiones dactilares genera para la protección de datos personales no pocos problemas, algunos de los cuales señalamos a continuación.

Aunque las impresiones dactilares presentan un alto índice de *precisión*, pueden fallar debido a limitaciones relacionadas con la información (baja calidad de los datos o proceso de adquisición no consistente) o la representación (rasgos seleccionados o calidad de los algoritmos de extracción). Todo lo cual puede dar lugar a falsos rechazos o a falsas correspondencias.

También al *impacto*: la irreversibilidad del proceso puede reducir la posibilidad de un individuo para ejercer sus derechos o invalidar las decisiones adoptadas basándose en una identificación falsa. El confiar en la precisión de la toma de huellas dactilares puede hacer más difícil rectificar los posibles errores. Esto debe tenerse en cuenta al evaluar la proporcionalidad del tratamiento en relación con la decisión específica que deba adoptarse sobre la base de las impresiones dactilares. Debe también mencionarse que la falta de medidas de seguridad puede dar lugar a la usurpación de identidad, que puede tener un fuerte impacto para el individuo.

En cuanto a la *vinculación*: las impresiones dactilares proporcionan posibilidades de uso indebido, ya que los datos pueden estar vinculados con otras bases de datos. Esta posibilidad puede dar lugar a usos no compatibles con los fines originales. Existen algunas técnicas, como la biometría convertible o la codificación biométrica, que pueden utilizarse para reducir el riesgo.

El *consentimiento* es una cuestión esencial en el uso de las impresiones dactilares para usos distintos de los policiales. Las impresiones dactilares pueden ser copiadas fácilmente de las impresiones dactilares latentes e incluso fotografías, sin conocimiento del individuo. Por otra parte, los datos de

impresiones dactilares son muy estables con el tiempo y deben considerarse *irrevocables*.

IV. Parámetros para la justificación de una limitación al derecho a la intimidad conforme a la CDFUE: el principio de proporcionalidad

En opinión del Tribunal de Justicia, tanto el derecho al respeto de la vida privada y familiar como a la protección de datos de carácter personal pueden ser limitados. Ahora bien, en estos casos se debe atender a lo dispuesto en la propia CDFUE (artículo 52, apartado 1) al indicar que, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta, "deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás".

A. Prevista por ley: mandato de calidad

El requisito de la limitación establecida por ley no crea mayores inconvenientes pues, tanto en el asunto *Schwarz* como en el asunto *R. L*, ya vimos que la limitación se encuentra expresamente prevista en el DUE.

El DUE en esta materia "debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión".[28]

Esta base legal debe ser suficientemente clara en sus términos para proporcionar a los ciudadanos una indicación adecuada de las condiciones y circunstancias en las que las autoridades están facultadas para recurrir a una medida de recogida de datos. Debe indicar con una claridad razonable el alcance y las modalidades de ejercicio de la correspondiente facultad discrecional conferida a las autoridades públicas, a fin de garantizar a los particulares el mínimo grado de protección que le confiere el Estado de Derecho en una sociedad democrática. Además, la legalidad requiere salvaguardias adecuadas

[28] STJ de 8 de abril de 2014, *Digital Rights Ireland y otros,* asuntos acumulados C 293/12 y C 594/12, [ECLI:EU:C:2014:238], apartado 54

para garantizar que se respete, en particular, el derecho individual reconocido en el artículo 8 (CDFUE).

En este punto se produce una clara convergencia en el *espacio público europeo* entre la jurisprudencia del Tribunal de Justicia -en el alcance dado a los artículos 7 y 8 (CDFUE)-, el TEDH -en su interpretación del artículo 8.1 (CEDH)[29], y la jurisprudencia constitucional.[30]

B. La "esencia" del derecho fundamental a la intimidad y a la protección de los datos personales

El Tribunal de Justicia interpreta que la información proporcionada por las impresiones dactilares "no permite, por sí sola, obtener una visión general de la vida privada y familiar de los interesados". En estas circunstancias, la limitación que supone la obligación de integrar dos impresiones dactilares en el medio de almacenamiento de los documentos de identidad "no menoscaba el contenido esencial de los derechos fundamentales recogidos en los artículos 7 y 8 (CDFUE)."[31]

C. Principio de proporcionalidad

El principio de proporcionalidad, según Luxemburgo, exige que los actos de las Instituciones de la UE "sean adecuados para lograr los objetivos legítimos

[29] STEDH de 1 de julio de 2008, *Liberty y otros c. Reino Unido*, [Demanda no 58243/00], apartados 62 y 63; STEDH de 4 de mayo de 2000, *Rotaru c. Rumanía* [Demanda no 28341/95], apartados 57 a 59, y STEDH de 4 de diciembre de 2008, *S. y Marper c. Reino Unido* [Demandas nº 30562/2004 y 30566/2004], apartados 99).

[30] A modo de ejemplo la doctrina constitucional española la cual sostiene que, "la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas –unas veces– de predeterminación normativa y –otras– de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares" (STC 76-2019, de 22 de mayo, FJ 8).

[31] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartados 80-81. Véase también STJ de 21 de junio de 2022, *Ligue des droits humains*, asunto C 817/19, [ECLI:EU:C:2022:491], apartado 120.

perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos".[32]

Más concretamente, las excepciones a la protección de los datos personales y las limitaciones de esta última operan dentro del marco de lo estrictamente necesario, entendiéndose que, cuando se ofrezca una elección entre varias medidas adecuadas para la consecución de los objetivos legítimos perseguidos, deberá recurrirse a la menos onerosa de ellas. Además, no puede perseguirse un objetivo de interés general sin tener en cuenta que tal objetivo debe conciliarse con los derechos fundamentales a los que afecta la medida, efectuando una "*ponderación equilibrada*" entre, por un lado, el objetivo de interés general y, por otro, los derechos en cuestión, para garantizar que los inconvenientes causados por esa medida no sean desmesurados en relación con los objetivos perseguidos. De este modo, la posibilidad de justificar una limitación a los derechos garantizados en los artículos 7 y 8 (CDFUE) "*debe apreciarse midiendo la gravedad de la injerencia que implica tal limitación y verificando que la importancia del objetivo de interés general perseguido por dicha limitación guarda relación con esa gravedad*".[33]

Como señala la doctrina, la dimensión constitucional del algoritmo debe abordarse en relación con el sistema de derechos constitucionales, que no puede renunciar a la garantía de los derechos en virtud de que su lesión se produzca a través de procedimientos informáticos mediante algoritmos. El algoritmo no deja de ser un instrumento destinado a una finalidad concreta y utilizado para mejorar procesos y obtener rendimientos de diversa naturaleza. Esa finalidad debe ser compatible con la constitución, como también deben serlo los algoritmos que se diseñan para conseguirla (BALAGUER CALLEJÓN: 2023, p. 34).

[32] STJ de 8 de abril de 2014, *Digital Rights Ireland y otros,* asuntos acumulados C 293/12 y C 594/12, [ECLI:EU:C:2014:238], apartado 46.

[33] STJ de 22 de noviembre de 2022, *Luxembourg Business Registers*, asuntos acumulados C 37/20 y C 601/20 [ECLI:EU:C:2022:912], apartado 66; STJ de 8 de diciembre de 2022, *Orde van Vlaamse Balies y otros*, asunto C 694/20 [ECLI:EU:C:2022:963], apartado 42; y STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 83. Sin resaltar en el original.

1. La limitación debe perseguir objetivos de interés general (legítimos) reconocidos por la UE

En cuanto al objetivo de interés general, el Reglamento nº 2252/2004 -interpretado a la luz de sus considerandos 2 y 3- se desprende que persigue concretamente dos objetivos precisos: el primero es prevenir la falsificación de pasaportes y el segundo impedir su uso fraudulento, esto es, su uso por personas que no sean su legítimo titular.[34] Al perseguir tales objetivos, dicha disposición pretende por tanto impedir, en particular, la entrada ilegal de personas en el territorio de la UE.[35]

En el mismo sentido se expresó el Abogado General Mengozzi al sostener que, dicho objetivo general, es proteger las fronteras exteriores mediante la aplicación de una política de gestión integrada. La inclusión en un pasaporte de las impresiones dactilares almacenadas en un soporte protegido pretende hacer más fiable el vínculo entre el documento y su titular, con lo cual dificulta su falsificación y su utilización fraudulenta y, en consecuencia, la inmigración ilegal. Por otro lado, la actuación del legislador era de gran importancia desde el punto de vista del establecimiento progresivo de un espacio de seguridad, libertad y justicia, y por la inexistencia de control en las fronteras interiores de la UE.[36]

En cuanto al Reglamento 2019/1157, según la Abogada General Medina, pretende facilitar el derecho de libre circulación de los ciudadanos de la UE (cfr. artículo 45, CDFUE)[37] haciendo más fiables los documentos de identidad nacionales en términos de autenticidad y de identidad. La falta de homogeneidad en los formatos y elementos de seguridad de los documentos de identidad nacionales incrementa el riesgo de falsificación y falsedad documental, cuya prevención constituye, por ende, un objetivo de ese Reglamento como manera

[34] Véase STJ del 16 de abril 2015, *Willems*, asuntos acumulados C-446/12 a C-449/12, [ECLI:EU:C:2015:238].
[35] STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartado 36.
[36] Conclusiones del Abogado General Paolo Mengozzi presentadas el 13 de junio de 2013, asunto C 291/12 [ECLI:EU:C:2013:401], *Schwarz*, apartado 44.
[37] La norma citada dice: "1. Todo ciudadano de la Unión tiene derecho a circular y residir libremente en el territorio de los Estados miembros. 2. Podrá concederse libertad de circulación y de residencia, de conformidad con lo dispuesto en los Tratados, a los nacionales de terceros países que residan legalmente en el territorio de un Estado miembro".

de promover la aceptación de tales documentos en Estados miembros distintos de los que los hayan expedido.[38]

A lo anterior, el Tribunal de Justicia agrega que los objetivos que persigue el Reglamento 2019/1157 "puede contribuir a la protección de la vida privada de los interesados y, más en general, a la lucha contra la delincuencia y el terrorismo". Además, tal medida permite responder a la necesidad que tiene todo ciudadano de la Unión de disponer de medios para identificarse de manera fiable y que tienen los Estados miembros de cerciorarse de que las personas que invocan derechos reconocidos por el DUE son realmente titulares de ellos. Por lo tanto, "los objetivos perseguidos por el Reglamento 2019/1157, en particular mediante la integración de dos impresiones dactilares en el medio de almacenamiento de los documentos de identidad, tienen especial importancia no solo para la Unión y los Estados miembros, sino también para los ciudadanos de la Unión".[39]

El Tribunal alemán que impulsó la cuestión prejudicial en el asunto *R. L* (2024), en este punto, plantea dudas. Si bien, en el asunto *Schwarz* (2013), el Tribunal de Justicia admitió que la lucha contra la entrada ilegal de nacionales de terceros países en el territorio de la UE es un objetivo reconocido por el DUE. Sin embargo, afirma, el documento de identidad no es primariamente un documento de viaje, como el pasaporte, y su objetivo es únicamente permitir la comprobación de la identidad de un ciudadano de la Unión en sus relaciones tanto con autoridades administrativas como con terceros particulares. Además, presenta dudas respecto a la proporcionalidad de la referida limitación. En su opinión, la solución adoptada en el citado asunto *Schwarz*, no es extrapolable al Reglamento 2019/1157 porque se refería a los pasaportes, cuya posesión, contrariamente a los documentos de identidad, es facultativa en Alemania y cuyo uso persigue un objetivo diferente. En cualquier caso, el Tribunal alemán remitente considera que la necesidad de llevar a cabo un "estricto control de

[38] Conclusiones del Abogada General Laila Medina presentadas el 29 de junio de 2023, asunto C 61/22 [ECLI:EU:C:2023:520], *R. L*, apartados 75-76. En el mismo sentido, STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 87.
[39] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartados 119-120.

proporcionalidad" se deriva también del artículo 9, apartado 1, del Reglamento (UE) 2016/679[40].[41]

En efecto, la norma citada titulada "Tratamiento de categorías especiales de datos personales" sostiene que, quedan prohibidos, "el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, *datos biométricos dirigidos a identificar de manera unívoca a una persona física*, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".[42]

La doctrina, por su parte, ha resaltado en su comentario al asunto *R. L* que el documento de identidad cumple la función de documento de viaje únicamente para los viajes entre Estados miembros de la UE, para la entrada en un Estado miembro procedente de un tercer país y para la salida a terceros Estados con los que existan acuerdos en vigor que prevean su aceptación como documento de viaje. La función principal del documento de identidad es, por tanto, servir de prueba a su titular de la identidad y ciudadanía. La inclusión de datos biométricos no parecería esencial para mejorar la función del documento consistente en identificar a su titular, si se considera que los Estados pueden seguir aceptando documentos distintos de los documentos de viaje a efectos de prueba de identidad (cfr. Preámbulo, punto 12, Reglamento 2019/1157), como las licencias de conducir que no contienen datos biométricos[43] (LANG: 2024, p. 24).

2. La limitación debe ser idónea para lograr el objetivo de interés general reconocido por la UE

[40] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).
[41] *Ídem*, apartados 33-36.
[42] Sin resaltar en el original.
[43] La UE estableció un modelo uniforme con la Directiva 2006/126/CE del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, sobre el permiso de conducción (*DO L 403 de 30.12.2006, p. 18/60*), sin prever la inclusión de datos biométricos. Se trata de un documento que en algunos Estados miembros cumple la función de documento de identidad.

El demandante en el asunto *Schwarz* (2013) niega que la recogida obligatoria de impresiones dactilares de los ciudadanos de la Unión que deseen obtener un pasaporte constituya un medio adecuado para realizar el objetivo perseguido, y duda de que contribuya de forma efectiva a proteger las fronteras exteriores. En esencia, sostiene que el método biométrico escogido es particularmente insatisfactorio y tiene, en todo caso, una utilidad limitada para los ciudadanos de la Unión respecto de los que no sea posible efectuar la recogida por motivos de enfermedad, lesiones o quemaduras. Añade que el citado método no puede garantizar la realización del objetivo perseguido por la fragilidad intrínseca del chip de almacenamiento, cuya vida útil es mucho más breve que la vigencia del pasaporte. Por último, dicho método presenta, según el demandante, una tasa de error importante y no es suficientemente seguro para garantizar la existencia de un vínculo absolutamente fiable entre el titular legítimo del pasaporte y el propio documento.[44]

La conservación de impresiones dactilares en un dispositivo de almacenamiento dotado de fuertes medidas de seguridad -en palabras del Tribunal de Justicia- implica una "*sofisticación técnica*", de modo que tal conservación puede reducir el riesgo de falsificación de pasaportes y facilitar la tarea de las autoridades encargadas de examinar la autenticidad de los mismos en las fronteras.[45] Desde este punto de vista, "no es determinante que dicho método no sea totalmente fiable". Aunque el mismo no excluya completamente las admisiones de personas no autorizadas, "basta con que reduzca considerablemente el riesgo de tales admisiones que existiría si ese mismo método no fuera utilizado".[46]

Consideraciones similares se repiten en el asunto *R. L* (2024) donde se afirma que, "aun considerando que el número de documentos de identidad fraudulentos fuera reducido, el legislador de la Unión no estaba obligado a esperar a que ese número aumentara para adoptar medidas dirigidas a prevenir el riesgo de utilización de tales documentos, sino que podía, en aras del control

[44] Véase Conclusiones del Abogado General Paolo Mengozzi presentadas el 13 de junio de 2013, asunto C 291/12 [ECLI:EU:C:2013:401], *Schwarz*, apartado 47.
[45] STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartado 41.
[46] *Ídem*, apartado 43.

de los riesgos, anticiparse a esa evolución, siempre que se observaran los demás requisitos relativos al respeto del principio de proporcionalidad".[47]

Por otra parte, en Luxemburgo defienden que si bien es cierto que la aplicación del método de verificación de identidad mediante impresiones dactilares puede dar lugar excepcionalmente al rechazo –indebido– de personas autorizadas, no lo es menos que la falta de concordancia de las impresiones dactilares del poseedor del pasaporte con los datos integrados en ese documento no significa (cfr. artículo 4, apartado 3, párrafo segundo, Reglamento nº 2252/2004), que se vaya a denegar automáticamente al interesado su entrada en el territorio de la UE. La única consecuencia de esa falta de concordancia será atraer la atención de las autoridades competentes sobre el interesado, y la realización de un control en profundidad para acreditar su identidad de manera definitiva.

La toma y conservación de impresiones dactilares, que prevé el artículo 1, apartado 2, del Reglamento nº 2252/2004 son, por lo tanto -según el Tribunal de Justicia-, "idóneas para alcanzar los objetivos perseguidos por este Reglamento y, por tanto, el objetivo de impedir la entrada ilegal de personas en el territorio de la Unión".[48]

El mismo criterio sobre la idoneidad de la medida se sigue en el asunto *R. L* (2024) donde el Tribunal de Justicia sostiene que "la integración de dos impresiones dactilares completas en el medio de almacenamiento de los documentos de identidad es idónea para alcanzar los objetivos de interés general de lucha contra la producción de documentos de identidad falsos y la suplantación de identidad, así como de interoperabilidad de los sistemas de verificación, invocados por el legislador de la Unión para justificar dicha medida".[49] Entre otras razones porque "el recurso a las impresiones dactilares completas permite garantizar una compatibilidad con todos los sistemas automatizados de identificación de las impresiones dactilares utilizados por los

[47] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 122.
[48] STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartado 45.
[49] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 89.

Estados miembros, aun cuando tales sistemas no recurran necesariamente al mismo mecanismo de identificación".[50]

3. Necesidad de recurrir a la medida en cuestión para alcanzar los objetivos de interés general perseguidos

En lo que se refiere al examen del carácter necesario de la recogida y almacenamiento de las impresiones dactilares, el legislador -afirma el Tribunal de Justicia- está obligado concretamente a verificar si se pueden concebir medidas que vulneren en menor medida los derechos reconocidos por los artículos 7 y 8 (CDFUE), sin dejar por ello de contribuir eficazmente a los objetivos de la normativa controvertida.[51]

En este contexto, con respecto al objetivo de proteger los pasaportes contra su uso fraudulento, debe examinarse, en primer término, si la vulneración que supone la medida de tomar impresiones dactilares "no va más allá de lo necesario para lograr ese objetivo". Esta recolección consiste únicamente en captar la impresión dactilar de dos dedos, los cuales están normalmente a la vista de los demás, de modo que "no se trata de una operación que revista un carácter íntimo. Tal operación tampoco supone un inconveniente físico o psíquico particular para el interesado, al igual que sucede con la toma de su imagen facial".[52]

La toma de las impresiones dactilares se añade a la toma de la imagen facial. No obstante, la acumulación de dos operaciones destinadas a la identificación de las personas no puede considerarse *a priori* que suponga, en sí misma, una vulneración más grave de los derechos reconocidos por los artículos 7 y 8 (CDFUE) que si tales operaciones fueran consideradas aisladamente.[53]

---

[50] *Ídem*, apartado 92.
[51] STJ de 9 de noviembre de 2010, *Volker und Markus Schecke y Eifert*, asuntos acumulados C 92/09 y C 93/09 [ECLI:EU:C:2010:662], apartado 86.
[52] STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartado 48.
[53] El Tribunal de Justicia señala que "la única alternativa real a la toma de las impresiones dactilares que se ha expuesto en el procedimiento ante el Tribunal de Justicia es la captación de una imagen del iris del ojo. Ahora bien, nada en dicha documentación indica que este último procedimiento vulnere en menor medida los derechos reconocidos por los artículos 7 y 8 de la Carta que la toma de las impresiones dactilares". Además, en cuanto a la eficacia de estos dos últimos métodos, "consta que el grado de desarrollo tecnológico del basado en el reconocimiento del iris es menor que el del basado en las impresiones dactilares. Por otra parte, el

Además, para verse justificado por un objetivo de esta naturaleza, es preciso asimismo que el artículo 1, apartado 2, del Reglamento nº 2252/2004 no implique un tratamiento de las impresiones dactilares tomadas que vaya más allá de lo necesario para lograr ese objetivo. A este respecto, se ha de señalar que el legislador "*debe asegurarse de que existen garantías específicas destinadas a proteger eficazmente tales datos contra los tratamientos inapropiados y abusivos*".[54]

En el sentido anterior, el artículo 4, apartado 3, del Reglamento nº 2252/2004 dispone expresamente que las impresiones dactilares sólo podrán utilizarse con el único fin de verificar la autenticidad del pasaporte y la identidad de su titular. Además, se garantiza la protección contra el riesgo de lectura de los datos que contengan impresiones dactilares por personas no autorizadas. A este respecto, del artículo 1, apartado 2, del Reglamento nº 2252/2004 se desprende que los correspondientes datos se conservan en un dispositivo de almacenamiento integrado en el pasaporte y dotado de fuertes medidas de seguridad. Dado que el citado Reglamento no contempla ninguna otra forma ni ningún otro medio de conservación de las impresiones dactilares, "*no puede ser interpretado*" -como pone de relieve el considerando 5 del Reglamento nº 444/2009[55]-, "*en el sentido de que ofrece, como tal, una base jurídica a una eventual centralización de los datos recabados en su virtud o a la utilización de los datos con fines distintos al de impedir la entrada ilegal de personas en el territorio de la Unión*".[56]

reconocimiento del iris es un procedimiento sensiblemente más oneroso, en la actualidad, que el de la comparación de impresiones dactilares y, por ello, menos apto para un uso generalizado" (STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartados 51 y 52).

[54] STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartado 55, donde se sigue la STEDH de 4 de diciembre de 2008, *S. y Marper c. Reino Unido* [Demandas nº 30562/2004 y 30566/2004], apartado 103. Sin resaltar en el original.

[55] Reglamento (CE) nº 444/2009 del Parlamento Europeo y del Consejo, de 28 de mayo de 2009, por el que se modifica el Reglamento (CE) nº 2252/2004 del Consejo sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros

[56] STJ de 17 de octubre de 2013, *Schwarz*, asunto C 291/12 [ECLI:EU:C:2013:670], apartado 61. Sin resaltar en el original.

V. El impacto global de la recogida y almacenamiento de las impresiones dactilares en la población. El principio de minimización de datos

En su presentación prejudicial el Tribunal alemán remitente en el asunto *R. L* (2024) considera que el artículo 3, apartado 5, del Reglamento 2019/1157 no respeta el *principio de minimización de datos* (cfr. artículo 5, Reglamento (UE) 2016/679), del que se desprende que la toma y la utilización de datos personales deben ser adecuadas, pertinentes y limitadas a lo necesario en relación con los fines para los que son tratados. Si bien, se afirma, permite favorecer la interoperabilidad de los diferentes tipos de sistemas, la recogida de dos impresiones dactilares completas, y no solamente de los puntos característicos de esas impresiones, aumenta también la cantidad de datos personales almacenados y, por lo tanto, el riesgo de suplantación de identidad en caso de filtración de datos. Añade que este riesgo no es insignificante, ya que los chips electrónicos utilizados en los documentos de identidad podrían ser leídos por escáneres no autorizados.[57]

Como lo señala la Abogada General Medina, en el caso del Reglamento 2019/1157 es preciso tener en cuenta el impacto global en la población de la UE, cuya obligación de incluir una imagen de sus impresiones dactilares en los documentos de identidad de nueva expedición puede afectar a hasta un 85 % de los ciudadanos de la Unión, dado el carácter obligatorio de esos documentos en la mayoría de los Estados miembros.[58]

Es cierto -destacan en Luxemburgo- que la evaluación de impacto realizada por la Comisión (cfr. Dictamen 7/2018) que acompañaba a la propuesta que dio lugar al Reglamento 2019/1157 indicó que debía preferirse la opción de no hacer obligatoria la integración de dos impresiones dactilares en el medio de almacenamiento de los documentos de identidad.[59] Sin embargo, destaca el Tribunal de Justicia que, aunque el Parlamento y el Consejo estén obligados a tener en cuenta las evaluaciones de impacto de la Comisión, “no están

[57] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 40.
[58] Conclusiones del Abogada General Laila Medina presentadas el 29 de junio de 2023, asunto C 61/22 [ECLI:EU:C:2023:520], *R. L*, apartado 80.
[59] Véase STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 100.

vinculados por su contenido, en particular, por lo que respecta a las apreciaciones que figuran en ellas".[60] En consecuencia, el mero hecho de que el legislador de la Unión haya adoptado una medida distinta y, en su caso, más restrictiva que la recomendada al término de la evaluación de impacto no demuestra que haya rebasado los límites de lo que era necesario para alcanzar el objetivo perseguido.[61]

Por otro lado, se interpreta que la integración de una impresión dactilar completa es necesaria para la *interoperabilidad* de los sistemas de verificación de los documentos de identificación, lo que constituye uno de los objetivos esenciales perseguidos. En efecto, como se desprende del citado Dictamen 7/2018 (apartado 47) y como subraya también el tribunal remitente, los Estados miembros utilizan diferentes tecnologías de identificación de impresiones dactilares, de modo que el hecho de integrar en el medio de almacenamiento del documento de identidad únicamente algunas de las características de una impresión digital tendría como efecto comprometer la consecución del objetivo de interoperabilidad de los sistemas de verificación de los documentos de identificación perseguido por el Reglamento 2019/1157.[62]

La jurisprudencia de Luxemburgo ha interpretado el principio de minimización de datos afirmando que, conforme al mismo, "el responsable del tratamiento está obligado a limitar a lo estrictamente necesario, a la luz del objetivo perseguido con el tratamiento, el período de recogida de los datos personales de que se trate".[63] Cuanto más tiempo se conservan estos datos -se afirma-, más importantes son las consecuencias sobre los intereses y sobre la vida privada del interesado y mayores las exigencias relativas a la licitud de la conservación de tales datos.[64] Puede ocurrir incluso que un tratamiento inicialmente lícito de datos puede devenir, con el tiempo, incompatible con lo

[60] Véase STJ de 21 de junio de 2018, *Polonia c. Parlamento y Consejo*, asunto C 5/16 ECLI:EU:C:2018:483], apartado 159.
[61] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 102. En el mismo sentido, STJ de 4 de mayo de 2016, *Pillbox 38*, asunto C 477/14 [ECLI:EU:C:2016:324], apartado 65.
[62] *Ídem*, apartado 104.
[63] STJ de 24 de febrero de 2022, *Valsts ieņēmumu dienests* (Tratamiento de datos personales con fines fiscales), asuntos acumulados C-175/20 [ECLI:EU:C:2022:124], apartado 79.
[64] STJ de 7 de diciembre de 2023, *SCHUFA Holding* (Exoneración del pasivo insatisfecho), asuntos acumulados C 26/22 y C 64/22 [ECLI:EU:C:2023:958], apartado 95.

dispuesto en el nombrado artículo 5 “cuando esos datos ya no sean necesarios en relación con los fines para los cuales fueron recogidos o tratados ulteriormente y que dichos datos deben suprimirse cuando se hayan cumplido esos fines”.[65] Consiguientemente, teniendo en cuenta el principio de minimización de datos, el responsable del tratamiento “*no puede proceder, de manera generalizada e indiferenciada, a la recogida de datos personales y que debe abstenerse de recoger datos que no sean estrictamente necesarios en relación con los fines del tratamiento*”.[66]

La lógica subyacente en este principio indica que es necesario limitarse a la recopilación de datos personales necesarios para lograr el propósito legítimo, eliminando aquellos que no sean necesarios o no cumplan con ese propósito. El propio concepto de minimización de datos resulta incompatible con las técnicas de análisis de *big data* y *machine learning*, que en un principio requieren una enorme cantidad de datos para ser procesados. Se ha visto que el valor de los datos en la economía digital representa un valor latente, que puede ser explotado plenamente no en el momento de la recopilación, sino cuando los datos se utilizan, reutilizan y combinan con otros datos para una variedad de propósitos (MOBILO: 2021, pp. 172-175).

VI. Ponderando entre la gravedad de la injerencia en los derechos fundamentales afectados y los objetivos perseguidos por dicha medida.

En el asunto *R. L.* (2024), el Tribunal de Justicia aprecia directamente la gravedad de la injerencia causada por una limitación de los derechos garantizados en los artículos 7 y 8 (CDFUE). Ello implica tener en cuenta la naturaleza de los datos personales de que se trate, en particular el carácter potencialmente sensible de esos datos, así como la naturaleza y el modo concreto del tratamiento de los datos, especialmente el número de personas que tienen acceso a ellos y el modo en que acceden. En su caso, también debe

[65] STJ de 20 de octubre de 2022, *Digi*, asunto C 77/21 [ECLI:EU:C:2022:805], apartado 54.
[66] STJ de 24 de febrero de 2022, *Valsts ieņēmumu dienests* (Tratamiento de datos personales con fines fiscales), asuntos acumulados C 175/20 [ECLI:EU:C:2022:124], apartado 74. Sin resaltar en el original.

tomarse en consideración la existencia de medidas para prevenir el riesgo de que tales datos sean objeto de tratamientos abusivos.

Se prevé que la limitación del ejercicio de los derechos garantizados en los artículos 7 y 8 (CDFUE) resultante del Reglamento 2019/1157, puede afectar a un gran número de personas. Número que la Comisión, en su evaluación de impacto, estimó en 370 millones de habitantes de los 440 millones con que contaba entonces la UE.

Las impresiones dactilares, en tanto que datos biométricos, son particularmente sensibles por su naturaleza y gozan, como se desprende del considerando 51 del Reglamento (UE) 2016/679, de una protección específica en el DUE. Sin embargo, se precisa, la recogida y el almacenamiento de dos impresiones dactilares completas solo están autorizados por el Reglamento 2019/1157 "con el fin de integrar dichas impresiones dactilares en el medio de almacenamiento de los documentos de identidad".[67] Una vez realizada esa integración y recogido el documento de identidad por el interesado, "*las impresiones dactilares recogidas se conservan únicamente en el medio de almacenamiento de dicho documento, el cual, en principio, se halla físicamente en poder del interesado* (cfr. artículo 3, apartado 5, en relación con el artículo 10, apartado 3, ambos del Reglamento 2019/1157)".[68]

Además, el Reglamento 2019/1157 establece un conjunto de *garantías* dirigidas a limitar los riesgos de que, al aplicarlo, se recojan o utilicen datos personales para fines distintos de la consecución de los objetivos que persigue, y ello no solo en lo referente a las operaciones de tratamiento de datos personales que este Reglamento hace obligatorias, sino también en relación con los principales tratamientos de los que pueden ser objeto las impresiones dactilares integradas en el medio de almacenamiento de los documentos de identidad.[69]

En lo que respecta específicamente al almacenamiento de los datos, el considerando 21 del Reglamento 2019/1157 puntualiza expresamente que este no establece "una base jurídica para crear o mantener bases de datos a nivel

[67] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 108.
[68] Sin resaltar en el original.
[69] STJ de 21 de marzo de 2024, *R. L*, asunto C 61/22 [ECLI:EU:C:2024:251], apartado 110.

nacional para el almacenamiento de datos biométricos en los Estados miembros", pues se trata de una cuestión de Derecho nacional que tiene que cumplir con el DUE en materia de protección de datos, como tampoco establece "una base jurídica para la creación o el mantenimiento de una base de datos centralizada a nivel de la Unión".

Por otro lado, el artículo 10, apartado 3, de dicho Reglamento establece que esos identificadores biométricos deben mantenerse solo hasta la fecha de recogida del documento y, en cualquier caso, no más de 90 días después de la fecha de expedición del documento y precisa que, "superado este período, dichos identificadores biométricos deben ser suprimidos o destruidos inmediatamente".

De lo anterior resulta que, el Reglamento 2019/1157, "no permite que los Estados miembros traten los datos biométricos para fines distintos de los previstos en este Reglamento. Además, esa misma disposición *se opone a una conservación centralizada de impresiones dactilares* que vaya más allá del almacenamiento provisional de dichas impresiones a fines de personalización de los documentos de identidad".[70]

Esta limitación expresa que impone el Tribunal de Justicia a la conservación de los datos sensibles en cuestión se explica aplicando el ya citado principio de minimización de datos (cfr. artículo 5, Reglamento (UE) 2016/679).

VII. Algunas conclusiones

Los datos biométricos vimos pueden permitir distintas operaciones como la *autenticación-verificación*, la *identificación* o la *categorización* de las personas físicas y el *reconocimiento de las emociones* de las personas físicas.

La autenticación o verificación biométrica lleva a determinar si la persona propietaria del documento es la misma a quien se le emitió y cuyas imágenes están almacenadas en el propio documento. Ello mediante la comparación de dos imágenes, la del documento y la tomada en el momento de la autenticación a la persona. Esta operación no requiere la creación de bases de datos -y el Tribunal de Justicia excluye expresamente que puedan crearse en el contexto

[70] *Ídem*, apartados 112-113. Sin resaltar en el original.

referido a partir de los datos biométricos en pasaportes y documentos de identidad-, sino únicamente el acceso fuera de línea al medio de almacenamiento ubicado en el documento. Su "único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física".[71]

La identificación de los datos biométricos, por su parte, consiste en dar un nombre y una identidad, de otro modo desconocidos, a la persona a la que pertenecen los datos biométricos. Esta operación requiere la comparación de los datos biométricos con otros datos biométricos que pueden almacenarse en bases de datos. En palabras del Reglamento (UE) 2024/1689 sobre IA, se hace referencia al "reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual, como la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla, a fin de determinar la identidad de una persona *comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos de referencia, independientemente de que la persona haya dado o no su consentimiento*".[72]

Tanto en el asunto *Schwarz* (2013) como en el asunto *R. L* (2024) se aborda el primer aspecto -la autenticación de datos biométricos-, pero las consecuencias de la conclusión a la que llegan en Luxemburgo no ignoran la potencial utilización de algoritmos vía IA para la identificación biométricas de personas. En efecto, alertando que en modo alguno podrían utilizarse los datos biométricos de pasaportes y documentos de identidad para generar las bases de datos necesarias para que la IA actúe. El Tribunal de Justicia deja en claro que ese no es el fin legítimo perseguido por el DUE analizado. Cualquier intento de avanzar más allá de la frontera de la verificación -en las circunstancias apuntadas-, debe considerarse una violación a los artículos 7 y 8 (CDFUE) comprometiendo, entre otros principios fundamentales, el de minimización de datos. Se descarta que el DUE citado pueda utilizarse como fundamento jurídico para "*una conservación centralizada de impresiones dactilares* que vaya más

[71] Cfr. Considerando 15 del Reglamento (UE) 2024/1689.
[72] *Ídem*.

allá del almacenamiento provisional de dichas impresiones a fines de personalización de los documentos de identidad".[73]

No se trata de una interpretación extraña la *espacio público europeo*. En su momento, el Consejo Constitucional francés declaro inconstitucional la Ley relativa a la protección de la identidad.[74] En apoyo a esta decisión se sostuvo que, el tratamiento de datos de carácter personal previsto, estaba destinado a recopilar los datos relativos de la "cuasi-totalidad de la población de nacionalidad francesa". Los datos biométricos registrados en este fichero, especialmente las huellas digitales, eran por sí mismas susceptibles de ser vinculadas a rastros físicos dejados involuntariamente o recopilados sin su consentimiento, lo cual los convertía en particularmente sensibles. Las características técnicas de este fichero permitía, además, su consulta con fines distintos a la verificación de la identidad de una persona ya que, las disposiciones de la ley impugnada, la autorizaban con otros fines de policía administrativa o judicial.[75] En consecuencia, se interpretó que las disposiciones impugnadas eran contrarias -por no poder ser consideradas como proporcionadas- al derecho al respeto de la vida privada constitucionalmente tutelado.[76]

VIII. Bibliografía

BALAGUER CALLEJÓN F. (2022). La Constitución del algoritmo. Fundación Giménez Abad, colección estudios nº 9, Zaragoza, pp. 206.

BALAGUER CALLEJÓN F. (2023). "La constitución del algoritmo. El difícil encaje de la constitución analógica en el mundo digital". Derecho Público de la Inteligencia Artificial, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, pp. 29-56.

[73] *Ídem*, apartados 112-113. Sin resaltar en el original.
[74] En su artículo 5 preveía el tratamiento de datos de carácter personal facilitando la recopilación y la conservación de los datos solicitados para la expedición del pasaporte francés y del documento nacional de identidad (el estado civil y el domicilio del titular, su talla, el color de sus ojos, dos huellas digitales y su fotografía). Asimismo, el artículo 10 permitía a los agentes individualmente designados y debidamente habilitados de los servicios de la policía y de la gendarmería nacional, acceder a la base datos prevista.
[75] Consejo Constitucional francés, sentencia de 22 de marzo de 2012, nº 2012-652 DC, considerandos 9 y 10.
[76] Considerando 11.

BARONA VILAR S. (2024). “Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale”. Actualidad Jurídica Iberoamericana, nº 21, pp. 298-33.

BERGONZINI G. (2024). “Sicurezza della città, tecnologie digitali e intelligenza artificiale: tra regole europee, garanzie costituzionali e autonomia locale”. Federalismi.it - Rivista di Diritto Pubblico Italiano, Comparato, Europeo, nº 25 (23-10-2024), pp. 1-43.

BUSTOS GISBERT R. (2024). “El constitucionalista europeo ante la inteligencia artificial: reflexiones metodológicas de un recién llegado”. Revista Española de Derecho Constitucional, nº 131, pp. 149-178.

CASTELLANO P. S. Y FERRER X. D. (2022). “Límites y garantías constitucionales frente a la identificación biométrica”. Revista de los Estudios de Derecho y Ciencia Política-Universitat Oberta de Catalunya, nº 35.

CASTELLANOS CLARAMUNT J. (2023). “Sobre los desafíos constitucionales ante el avance de la inteligencia artificial. Una perspectiva nacional y comparada”. Revista de Derecho Político-UNED, nº 118, pp. 261-287.

COTINO HUESO L. (2023). “Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos”. Derecho Público de la Inteligencia Artificial, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, pp. 347-402.

DE SANTIS V. (2024). “Identità e persona all’epoca dell’intelligenza artificiale: riflessioni a partire dall’IA Act”. Federalismi.it - Rivista di Diritto Pubblico Italiano, Comparato, Europeo, nº 19 (07-08-2024), pp. 137-298.

FAINI F. (2023). “Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina”. Federalismi.it - Rivista di Diritto Pubblico Italiano, Comparato, Europeo, nº 23 (25-01-2023), pp. 1-30.

FASAN M. (2022). “I principi costituzionali nella disciplina dell’Intelligenza Artificiale. Nuove prospettive interpretative”. Diritto Pubblico Comparato ed Europeo-DPCE online, nº 1, pp. 181-199.

GARRIGA DOMÍNGUEZ A. (2024). "Los derechos ante los sistemas biométricos que incorporan inteligencia artificial". Derechos y Libertades, nº 51, pp. 117-149.

GONZÁLEZ PASCUAL M. (2014). "El TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland". Revista de Derecho Comunitario Europeo, nº 49, pp. 943-971.

LANG A. (2024). "La validità della carta di identità biometrica secondo la Corte di giustizia". Rivista.eurojus.it , nº 2, pp. 20-37.

MOBILIO G. (2021). Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative. Editoriale Scientifica, Collana Ricerche Giuridiche, Napoli, pp. 401.

MOLLO F. (2024). "Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale". Federalismi.it - Rivista di Diritto Pubblico Italiano, Comparato, Europeo, nº 28 (20-11-2024), pp. 91-129.

RALLO LOMBARTE A. (2017). "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet". Teoría y Realidad Constitucional-UNED, nº 39, pp. 583-610.

ROSSI DAL POZZO F. (2018). "La tutela dei dati personali nella giurisprudenza della Corte di giustizia". Federalismi.it - Relazione tenuta al I convegno annuale dell'Associazione italiana studiosi di diritto dell'Unione europea (AISDUE), Roma, 26-27 ottobre 2018., pp. 1-24.