# Dictamen del EDPB sobre el uso de sistemas de reconocimiento facial para agilizar el flujo de pasajeros en los aeropuertos

Nota informativa



*Categoría:*

# Nota informativa: Dictamen del EDPB sobre el uso de sistemas de reconocimiento facial para agilizar el flujo de pasajeros en los aeropuertos

**12 de junio 2024**

El 23 de mayo de 2024, el Comité Europeo de Protección de Datos (en adelante, "**EDPB**") adoptó el Dictamen 17/2024 sobre el uso del reconocimiento facial para agilizar el flujo de pasajeros en los aeropuertos. En este dictamen se realiza un análisis de la compatibilidad de este tratamiento de datos con el Reglamento General de Protección de Datos (RGPD), centrándose en aspectos clave como el almacenamiento de los datos biométricos, la minimización de datos, la protección de la privacidad desde el diseño y por defecto y las medidas de seguridad. A través de diferentes escenarios, el EDPB evalúa la seguridad y la privacidad de la tecnología de reconocimiento facial en el contexto aeroportuario, proporcionando orientación sobre cómo garantizar el cumplimiento normativo y proteger los derechos de los interesados.

## (I) RIESGOS ASOCIADOS AL USO DE LA TECNOLOGÍA DE RECONOCIMIENTO FACIAL

El Dictamen del EDPB se produce ante la solicitud de la Autoridad de Supervisión francesa (en adelante, "**Autoridad francesa**"), tras advertir que los modelos que se están probando actualmente en varios aeropuertos de la Unión Europea (UE) difieren de un Estado miembro a otro, lo que puede llegar a generar interpretaciones contradictorias entre las autoridades de control y producir consecuencias diferentes para los derechos y libertades fundamentales de los interesados en la UE.

En este sentido, el EDPB aclara que, sin perjuicio de la regulación en las legislaciones nacionales de los Estados miembros, el uso de tecnología de reconocimiento facial en aeropuertos conlleva varios riesgos para los derechos y libertades de los interesados:

- **(i)** **Los datos biométricos gozan de protección especial según el RGPD (art. 9)** ya que su tratamiento puede tener implicaciones significativas en la privacidad y seguridad de los interesados.
- **(ii)** **Falsos negativos, sesgos y discriminación** asociados al reconocimiento facial, lo que puede llevar a decisiones erróneas o injustas basadas en la tecnología.
- **(iii)** **El uso indebido de los datos biométricos, como la usurpación de identidad o la suplantación de identidad,** puede tener graves consecuencias para las personas.
- **(iv)** **Si el reconocimiento facial se realiza a distancia y sin la participación activa del interesado,** las personas pueden no ser completamente conscientes de dicho tratamiento y de los riesgos asociados.

Atendiendo a estos riesgos vinculados al uso de sistemas de reconocimiento facial, el EDPB subraya la importancia de evaluar cuidadosamente el impacto en la privacidad y los derechos fundamentales de las personas antes de su implementación.

## (II) ASPECTOS ESPECÍFICOS ABORDADOS EN RELACIÓN CON EL RGPD.

Este dictamen analiza el uso datos biométricos para agilizar el flujo de pasajeros en aeropuertos en puntos de control específicos centrándose en: **(i) si los datos están bajo el propio control del interesado y (ii) si están almacenados en una base de datos central.** En cualquiera de los casos, el EDPB prevé que el tratamiento de datos a través de estos sistemas requeriría que los interesados se inscriban activamente y den su consentimiento.

Además, el EDPB destaca la configuración del tratamiento de forma que sea compatible con los principios del tratamiento, especialmente, con los siguientes:

1. **Necesidad y proporcionalidad:** el uso de datos biométricos debe ser estrictamente necesario y proporcional para los fines del tratamiento. Se debe evaluar si existen soluciones menos intrusivas que puedan lograr el mismo objetivo con la misma eficacia.
2. **Limitación del plazo de conservación**: deberá limitarse un período de conservación que justifique que el plazo previsto es necesario para el fin determinado. En este sentido se recuerda que existen pasajeros con poca frecuencia y que lo más idóneo será la determinación de un período breve.
3. **Integridad y confidencialidad:** se deben implementar medidas de seguridad adecuadas que garanticen la confidencialidad y la integridad de la información, y eviten los accesos no autorizados o ilegales. Especialmente, en el caso de escenarios que conlleven un almacenamiento centralizado de datos biométricos, ya que supone un mayor riesgo respecto a los datos biométricos que se encuentren almacenados por el propio interesado.
4. **Protección de datos desde el diseño y por defecto** y **seguridad del tratamiento**: los responsables del tratamiento deberán implementar en los sistemas de reconocimiento facial las garantías y medidas de seguridad necesarias para cumplir de forma específica con los principios y la reducción de riesgos. Concretamente se especifica la implementación según el volumen de datos recabados, la extensión del tratamiento, y el período de conservación y accesibilidad a los datos.
5. **Evaluación de impacto en la protección de datos:** de forma previa al tratamiento de datos biométricos, se debe realizar una Evaluación de Impacto en la Protección de Datos (EIPD) para evaluar los posibles riesgos para los derechos y libertades de los individuos y garantizar el cumplimiento de las normativas de protección de datos.

Estos aspectos específicos del dictamen del EDPB proporcionan orientación sobre cómo abordar el uso de tecnología de reconocimiento facial en aeropuertos de manera compatible con las disposiciones del RGPD y en línea con la protección de los derechos de los individuos. En este sentido, en la siguiente tabla se muestra la compatibilidad de los diferentes escenarios con el RGPD:

| ESCENARIOS | Art. 5.1 e) | Art. 5.1 f) | Art. 24 | Art. 32 |
|---|---|---|---|---|
| Almacenamiento de la plantilla biométrica registrada solo en manos del individuo para su autenticación (Comparación 1:1) | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Almacenamiento centralizado de la plantilla biométrica inscrita de forma encriptada dentro del aeropuerto y con una clave/secreto únicamente en manos de los pasajeros para su autenticación (Comparación 1:1) | ✓ | ✓ | ✓ | ✓ |
| Almacenamiento centralizado de la plantilla biométrica en una base de datos dentro del aeropuerto bajo el control del gestor aeroportuario para su identificación (Comparación 1: N) | ✓ | ✗ | ✗ | ✗ |
| Almacenamiento centralizado de la plantilla biométrica en una nube bajo el control de la compañía aérea (Comparación 1: N) | ✗ | ✗ | ✗ | ✗ |

Algunos de los **controles propuestos por el EDPB** para los escenarios anteriormente descritos, y que pueden tenerse en cuenta para la elaboración de los análisis, son:

- Almacenamiento de los datos biométricos deberá ser controlado por los propios pasajeros, es decir, no solo que se implementen plazos por la entidad, si no que los interesados tengan la opción de suprimirlos.
- Mantenimiento de logs que corresponden al acceso de los datos de identificación y biométricos.
- Que las bases centrales de datos no se encuentren conectadas a la red. El mantenimiento y funcionamiento se realizará localmente dentro del propio aeropuerto.
- Indexación de las plantillas biométricas almacenadas para que se realice autenticación 1:1, además de garantizar que no existe correlación entre la identificación de los pasajeros y la encriptación.

En cualquier caso, el EDPB hace énfasis en que, a pesar de que algunos escenarios cumplan con los requisitos de los preceptos señalados del RGPD, **corresponde al responsable del tratamiento demostrarlo en cada caso con elementos de hecho y, además, dicha demostración deberá incluir la consideración de escenarios alternativos.**

## (III) CONCLUSIONES

En resumen, **el EDPB ha reflejado en este dictamen que el uso de tecnología de reconocimiento facial en aeropuertos puede ser compatible con el RGPD.** En este sentido, el EDPB recalca como requisitos esenciales:

- cumplir los principios de necesidad y proporcionalidad,
- obtener el consentimiento adecuado,
- mantener el control de los datos por parte de los individuos
- garantizar la seguridad y confidencialidad de los datos,
- y realizar una evaluación de impacto en la protección de datos.

Por lo tanto, **se puede concluir en la importancia de elaborar un sistema que analice la privacidad desde el diseño**, en el que se detecten las garantías necesarias para cumplir con la normativa, así como las medidas de seguridad necesarias para la minimización de riesgos.


Calle Serrano, 69.
28006 Madrid
www.ecija.com

**Área de Protección de Datos de ECIJA**
info@ecija.com
Telf: + 34 91.781.61.60