Dictamen 11/2024, sobre el uso del reconocimiento facial para agilizar el flujo de pasajeros de los aeropuertos [compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD]

Versión 1.1

Adoptado el 23 de mayo de 2024

Adoptado

Versión 1.1	28 de mayo de 2024	Corrección gramatical en el resumen (páginas 3 y 4) y apartados 77 y 90 del Dictamen
Versión 1.0	23 de mayo de 2024	Adopción del Dictamen

Resumen ejecutivo

La autoridad de control francesa solicitó al Comité Europeo de Protección de Datos que emitiera un dictamen sobre el uso de la tecnología de reconocimiento facial por parte de los operadores aeroportuarios y las compañías aéreas para la autenticación o identificación biométrica de los pasajeros a fin de agilizar el flujo de pasajeros en los aeropuertos.

Como observación preliminar, el Comité recuerda que el uso de datos biométricos y, en particular, de la tecnología de reconocimiento facial conlleva riesgos elevados para los derechos y libertades de los interesados. Se refiere al tratamiento de datos biométricos a los que se concede una protección especial en virtud del artículo 9 del RGPD. Antes de utilizar estas tecnologías, aunque se consideraran especialmente eficaces, los responsables del tratamiento deben evaluar el impacto en los derechos y libertades fundamentales de los interesados y considerar si unos medios menos intrusivos pueden alcanzar su objetivo legítimo del tratamiento.

El ámbito del presente Dictamen, conforme a la solicitud, se limita a la compatibilidad del tratamiento con el **artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD**, con el **fin específico de agilizar el flujo de pasajeros en los aeropuertos** en cuatro puntos de control concretos, a saber, los puntos de control de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros. El presente Dictamen no incluye un análisis completo y exhaustivo sobre el cumplimiento del RGPD por parte del responsable o responsables del tratamiento pertinentes en cada caso, así como de sus encargados del tratamiento, cuando proceda. Por lo tanto, el presente Dictamen se entiende sin perjuicio de un análisis jurídico y técnico caso por caso en función del tratamiento específico previsto por un responsable del tratamiento y las circunstancias. Además, el análisis de la base jurídica aplicable no entra en el ámbito de las cuestiones planteadas al Comité en la solicitud y, en consecuencia, en el presente Dictamen no se examina la validez del consentimiento para dicho tratamiento, de conformidad con los artículos 6, 7 y 9 del RGPD. Además, el Dictamen se entiende sin perjuicio de las restricciones al uso de datos biométricos establecidas en el Derecho de los Estados miembros.

En el presente Dictamen, el Comité evalúa la conformidad del tratamiento con las disposiciones del RGPD mencionadas en el contexto de **cuatro escenarios específicos**.

El **primer escenario** consiste en almacenar una plantilla biométrica registrada en manos de la persona, por ejemplo, en su dispositivo individual, bajo su control exclusivo, con el fin de autenticar (comparación 1:1) al pasajero a medida que avanza por los controles de seguridad aeroportuarios antes mencionados.

El Comité concluye que podría considerarse que las medidas elegidas cumplen el principio de necesidad si el responsable del tratamiento puede demostrar que no existen soluciones alternativas menos intrusivas que puedan lograr el mismo objetivo con la misma eficacia. Además, el carácter intrusivo del tratamiento puede contrarrestarse con la participación activa de los pasajeros, ya que su plantilla biométrica se conserva solo en sus manos, por ejemplo, en su dispositivo individual, bajo su solo control, y sus datos se eliminan poco después de que finalice el cotejo. Sobre esta base, el Comité concluye que el tratamiento previsto en el primer escenario **podría considerarse, en principio, compatible con el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD**, a reserva de la aplicación de las garantías adecuadas.

El Comité ha determinado las garantías que, como mínimo, deben aplicarse para una solución similar al primer escenario.

El **segundo escenario** consiste en la conservación centralizada, dentro del aeropuerto, de una plantilla biométrica registrada de forma cifrada con una clave o código secreto únicamente en manos del pasajero. Esto permite la autenticación de los pasajeros (comparación 1:1) a medida que pasan por los mencionados controles de seguridad aeroportuarios. El registro es válido durante un periodo determinado que, por ejemplo, podrá ser de hasta un año después del último vuelo realizado hasta la fecha de caducidad del pasaporte.

El Comité concluye que podría considerarse que el tratamiento cumple el principio de necesidad si el responsable del tratamiento puede demostrar que no existen soluciones alternativas menos intrusivas que permitan alcanzar el mismo objetivo con la misma eficacia. Además, el carácter intrusivo del tratamiento puede contrarrestarse con la participación activa del pasajero, ya que este tiene bajo su exclusivo control la clave o código secreto de sus datos biométricos cifrados. Suponiendo que el responsable del tratamiento aplique las garantías adecuadas, los riesgos para la seguridad derivados del uso de una base de datos centralizada en este escenario podrían mitigarse y el impacto negativo sobre los derechos y libertades fundamentales de los interesados podría considerarse proporcional al beneficio previsto. En cuanto al principio de limitación del plazo de conservación, no se ha facilitado al Comité ninguna información que justifique el largo plazo de conservación. A fin de lograr la compatibilidad con el artículo 5, apartado 1, letra e), del RGPD, en este escenario, los responsables del tratamiento deben poder justificar por qué el plazo de conservación previsto es necesario para el propósito en casos específicos. El Comité recomienda que los responsables del tratamiento prevean el plazo de conservación más breve posible, ofreciendo al mismo tiempo a los pasajeros la opción de fijar su plazo de conservación preferido. Sobre esta base, el Comité concluye que el tratamiento previsto en el segundo escenario **podría considerarse, en principio, compatible con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD**, a reserva de la aplicación de las garantías adecuadas.

El Comité ha determinado las garantías que, como mínimo, deben aplicarse para una solución similar al primer escenario.

El **tercer escenario** consiste en la conservación centralizada de una plantilla biométrica registrada en forma cifrada dentro del aeropuerto bajo el control del gestor del aeropuerto. Esto permite la identificación de los pasajeros (comparación 1: N) a medida que pasan por los mencionados controles de seguridad aeroportuarios. El plazo de conservación en este escenario suele ser de cuarenta y ocho horas y los datos se eliminan una vez que el avión ha despegado.

Dado que la conservación de los datos biométricos y de identificación se realiza en una base de datos central, si la confidencialidad de la base de datos se ve comprometida, puede implicar posteriormente el acceso a todo el conjunto de datos y podría permitir la identificación no autorizada o ilegal de pasajeros en otros entornos. La arquitectura de conservación centralizada bajo el control del gestor aeroportuario también hace que el pasajero pierda en mayor medida el control de sus datos. El Comité considera que puede lograrse un resultado similar a la agilización del flujo de pasajeros en los aeropuertos de una manera menos intrusiva y que el impacto negativo sobre los derechos y libertades fundamentales de los interesados que se derivaría de una violación de la seguridad de los datos en una base de datos centralizada de datos biométricos parece superar el beneficio previsto resultante del tratamiento. Por lo tanto, el tratamiento no puede cumplir los principios de necesidad y proporcionalidad. Sobre esta base, el Comité concluye que el tratamiento previsto en el tercer escenario **no puede ser compatible con el artículo 25 del RGPD**. **Tampoco sería conforme con el**

artículo 5, apartado 1, letra f), y el artículo 32 del RGPD, si un responsable del tratamiento se limitara a las medidas descritas en este escenario.

El **cuarto escenario** consiste en la conservación centralizada de una plantilla biométrica registrada en forma cifrada en la nube bajo el control de la compañía aérea o de su proveedor de servicios en la nube. Esto permite la identificación de los pasajeros (comparación 1: N) a medida que pasan por los mencionados controles de seguridad aeroportuarios. El plazo de conservación en este escenario podría durar tanto tiempo como el cliente tenga una cuenta en la compañía aérea.

Dado que la conservación de los datos biométricos y de identificación se realiza en una base de datos central en la nube, múltiples entidades podrían tener acceso a dichos datos, incluidos posiblemente proveedores ajenos al EEE. Los datos del pasajero se descifran cuando se usan y las claves están bajo el control de la compañía aérea o de sus encargados del tratamiento, lo que podría aumentar la superficie de exposición de la seguridad. Esta arquitectura centralizada de conservación también hace que el pasajero pierda en mayor medida el control de sus datos. Los datos también podrían conservarse durante un periodo de tiempo considerable, lo que los expone a mayores riesgos de violación de la seguridad y parece ir más allá de lo estrictamente necesario y proporcionado para los fines del tratamiento, a menos que se tomen otras medidas claras para mitigar los riesgos para las personas.

El Comité considera que puede lograrse un resultado similar de agilización del flujo de pasajeros en los aeropuertos de una manera menos intrusiva y que el impacto negativo sobre los derechos y libertades fundamentales de los interesados que podría derivarse de una violación de la seguridad de los datos en una base de datos centralizada de datos biométricos parece superar el beneficio previsto resultante del tratamiento. Por lo tanto, el tratamiento no puede cumplir los principios de necesidad y proporcionalidad. Sobre esta base, el Comité concluye que el tratamiento previsto en el cuarto escenario **no puede ser compatible con el artículo 25 del RGPD**. Además, **no cumpliría lo dispuesto en el artículo 5, apartado 1, letra e), del RGPD** sobre la base de la información de que dispone el Comité y **no cumpliría lo dispuesto en el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD** si un responsable del tratamiento se limitara a las medidas descritas en este escenario.

Índice

1 INTRODUCCIÓN....6
1.1 Resumen de los hechos....6
1.2 Admisibilidad de la solicitud de dictamen con arreglo al artículo 64, apartado 2, del RGPD 8
2 ÁMBITO y CONTEXTO DEL DICTAMEN....9
2.1 Ámbito del Dictamen....9
2.2 Nociones esenciales....12
3 Sobre el fundamento de la solicitud....15
3.1 Observaciones generales....15
3.2 Sobre la compatibilidad con el artículo 5, apartado 1, letras e) y f), y con los artículos 25 y 32 del RGPD....17
3.2.1 Escenario 1: conservación de la plantilla biométrica registrada únicamente en manos de la persona para su autenticación....17
3.2.2 Escenario 2: conservación centralizada de la plantilla biométrica registrada de forma encriptada dentro del aeropuerto y con una clave secreta únicamente en manos de los pasajeros, para la autenticación....26
3.2.3 Conservación centralizada de las plantillas biométricas registradas con fines de identificación....31
3.2.3.1 Escenario 3.1: Conservación centralizada en una base de datos dentro del aeropuerto, bajo el control del operador del aeropuerto....31
3.2.3.2 Escenario 3.2: conservación centralizada en una nube, bajo el control de la compañía aérea 35
4 CONCLUSIONES....38

El Comité Europeo de Protección de Datos

Visto el artículo 63 y el artículo 64, apartado 2, 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 (en lo sucesivo, el «**RGPD**»),

Visto el Acuerdo EEE, y en particular su anexo XI y su protocolo 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[1],

Vistos el artículo 10 y el artículo 22 del Reglamento interno del Comité Europeo de Protección de Datos (en lo sucesivo, el «**Comité**» o el «**CEPD**») (en lo sucesivo, el «**Reglamento interno del CEPD**»),

Considerando que:

1) La función principal del Comité consiste en garantizar la aplicación coherente del RGPD en todo el Espacio Económico Europeo (en lo sucesivo, el «**EEE**»). El artículo 64, apartado 2, del RGPD establece que cualquier autoridad de control (en lo sucesivo, «**AC**»), el presidente del Comité o la Comisión Europea podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen.

2) El dictamen del Comité será adoptado de conformidad con el artículo 64, apartado 3, del RGPD, leído en relación con el artículo 10, apartado 2, del Reglamento interno del Comité, en el plazo de ocho semanas a partir del momento en que el presidente y la AC competente hayan decidido que el expediente está completo. Habida cuenta de la complejidad del asunto, dicho plazo puede prorrogarse seis semanas por decisión de la presidenta.

ha aprobado el siguiente Dictamen:

1 INTRODUCCIÓN

1.1 Resumen de los hechos

1. El 16 de febrero de 2024, la autoridad de control francesa (en lo sucesivo, la «**AC FR**») solicitó al Comité que emitiera un dictamen sobre la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD del uso de la tecnología de reconocimiento facial por parte de los gestores aeroportuarios y las compañías aéreas para la autenticación o identificación biométricas de los pasajeros[2], con el fin de agilizar el flujo de pasajeros en los controles de seguridad aeroportuarios[3], la entrega de equipajes, el embarque y el acceso a la sala de pasajeros (excluidos el control fronterizo y

[1] Las referencias a los «**Estados miembros**» en el presente Dictamen deben entenderse como referencias a los «Estados miembros del EEE». Las referencias a la «Unión» o la «UE» en el presente Dictamen se entenderán hechas al «EEE».

[2] En el contexto del presente Dictamen, se entenderá por «**pasajero**» un interesado cuyos datos personales se traten con el fin específico descrito en el Dictamen. En lo sucesivo, en el presente Dictamen, los términos «pasajero» y «persona» se utilizan indistintamente.

[3] A efectos del presente Dictamen, por «**controles de seguridad aeroportuarios**» se entienden los controles de seguridad realizados bajo la responsabilidad del gestor aeroportuario a los que deben someterse los pasajeros para acceder desde la sala de salidas a la zona o puerta de embarque.

los controles realizados por las tiendas libres de impuestos) (en lo sucesivo, la «**solicitud**»). La AC FR adjuntó a su solicitud una descripción de los casos de uso típicos (anexo I).

2. En su solicitud, la AC FR observa que los modelos que se están probando actualmente en varios aeropuertos de la UE varían de un Estado miembro a otro, lo que posiblemente crea un riesgo de divergencia entre las interpretaciones de las AC y un riesgo de que se produzcan efectos diferentes para los derechos y libertades fundamentales de los interesados en la UE[4].

3. El Comité considera que, para dar una respuesta a la solicitud, deben responderse las siguientes preguntas:

4. **Pregunta 1**:

1.1. ¿Puede ser compatible con el **artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD** el uso de la tecnología de reconocimiento facial para la autenticación basada en datos biométricos **con el fin específico de agilizar el flujo de pasajeros en los aeropuertos** (controles de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros), en el caso de una arquitectura de conservación, en la que la plantilla biométrica de cada pasajero se conserva **solo en manos de la persona**, por ejemplo, localmente en su dispositivo individual, bajo su control exclusivo?

1.2. Si dicho tratamiento se considerase compatible con las disposiciones mencionadas, ¿qué garantías mínimas adecuadas serían necesarias, a la luz de los artículos 25 y 32 del RGPD?

Pregunta 2:

2.1. ¿Puede ser compatible con el **artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD** el uso de la tecnología de reconocimiento facial para la autenticación o identificación basadas en datos biométricos **con el fin específico de agilizar el flujo de pasajeros en los aeropuertos** (controles de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros), en el caso de una arquitectura de conservación **centralizada**, en la que la plantilla biométrica de cada pasajero se conserva en una base de datos central?:

2.1.1. ¿En una base de datos central dentro del aeropuerto, bajo el control del operador del aeropuerto, en forma cifrada, con una llave o código secreto exclusivamente en manos de la persona (por ejemplo, en su teléfono móvil), para su autenticación?

2.1.2. Si dicho tratamiento se considerase compatible, ¿qué garantías mínimas adecuadas serían necesarias, a la luz de los artículos 25 y 32 del RGPD?

2.2.1. ¿En una base de datos central del aeropuerto, bajo el control del gestor del aeropuerto, en forma cifrada, con las claves su poder, a efectos de identificación?

2.2.2. Si dicho tratamiento se considerase compatible, ¿qué garantías mínimas adecuadas serían necesarias, a la luz de los artículos 25 y 32 del RGPD?

[4] Solicitud, p. 1.

2.3.1. ¿En la nube, bajo el control de la compañía aérea o de su proveedor de servicios (encargado del tratamiento), en forma cifrada, con claves en poder de la compañía aérea o su proveedor de servicios, para su identificación?

2.3.2. Si dicho tratamiento se considerase compatible, ¿qué garantías mínimas adecuadas serían necesarias, a la luz de los artículos 25 y 32 del RGPD?

5. Después de que la AC FR considerara que el expediente estaba completo el 16 de febrero de 2024 y el presidente del Comité hiciera lo propio el 23 de febrero de 2024, la Secretaría distribuyó el expediente el 23 de febrero de 2024. El Presidente del Comité decidió, de conformidad con el artículo 64, apartado 3, del RGPD, leído en relación con el artículo 10, apartado 2, del Reglamento interno del CEPD, ampliar el plazo por defecto de ocho semanas en otras seis semanas debido a la complejidad del asunto.

1.2 Admisibilidad de la solicitud de dictamen con arreglo al artículo 64, apartado 2, del RGPD

6. El artículo 64, apartado 2, del RGPD establece que, en particular, cualquier AC podrá solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen.

7. El Comité considera que la solicitud remitida por la AC FR sobre la compatibilidad del uso de la tecnología de reconocimiento facial para la autenticación o identificación mediante biometría con el fin específico de agilizar el flujo de pasajeros en los aeropuertos se refiere a cuestiones «que producen efectos en más de un Estado miembro», ya que, como se explica en la solicitud[5], actualmente hay varios proyectos en fase de implantación en aeropuertos de los Estados miembros, y se estima que dicho uso aumentará en los próximos años. Los modelos que están probando en la actualidad los distintos aeropuertos y compañías aéreas varían significativamente de un Estado miembro a otro, lo que puede crear el riesgo de que, desde el punto de vista de la protección de datos, se produzcan efectos divergentes en más de un Estado miembro.

8. Asimismo, el Comité considera que la solicitud remitida por la AC FR tiene importantes consecuencias para la aplicación de los principios establecidos en el artículo 5, apartado 1, letras e) y f), del RGPD, y los requisitos aplicables a los responsables del tratamiento en virtud del artículo 25 del RGPD, así como los requisitos aplicables a los responsables y encargados del tratamiento en virtud del artículo 32 del RGPD. Por lo tanto, esta solicitud se refiere a un «asunto de aplicación general» en el sentido del artículo 64, apartado 2, del RGPD, ya que se refiere a la interpretación coherente de los principios de limitación del plazo de conservación [artículo 5, apartado 1, letra e), del RGPD] y de integridad y confidencialidad [artículo 5, apartado 1, letra f), del RGPD], así como a las nociones de protección de datos desde el diseño y por defecto (artículo 25 del RGPD) y de seguridad de los datos (artículo 32 del RGPD) para garantizar, entre otros aspectos, la aplicación coherente de dichas disposiciones en el EEE.

9. Cualquier posible posición divergente entre los Estados miembros sobre la interpretación del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD ampliaría el riesgo de que los operadores aeroportuarios y las compañías aéreas desarrollen proyectos de reconocimiento facial de manera no coherente. Dado que la AC FR ha demostrado la clara necesidad de una interpretación coherente de estas disposiciones en relación con la tecnología de reconocimiento facial para la autenticación o identificación biométrica de los pasajeros, con el fin de agilizar el flujo de pasajeros

[5] Solicitud, p. 3.

en los aeropuertos[6], el Comité considera que la solicitud está motivada, de conformidad con el artículo 10, apartado 3, del Reglamento interno del CEPD.

10. De conformidad con el artículo 64, apartado 3, del RGPD, el CEPD no emitirá un dictamen si ya ha emitido un dictamen sobre el mismo asunto[7]. El CEPD aún no ha proporcionado respuestas a las preguntas derivadas de la solicitud. Aunque las Directrices 3/2019 del CEPD sobre dispositivos de vídeo[8] ya proporcionan algunos elementos útiles sobre las medidas de seguridad que deben aplicarse al tratamiento de datos biométricos, no abordan todos los aspectos relativos a las cuestiones planteadas en la solicitud. Además, las orientaciones disponibles del CEPD, incluidas las Directrices 3/2019 del CEPD sobre dispositivos de vídeo, no proporcionan orientaciones específicas sobre los posibles elementos que deben verificarse en relación con la conservación centralizada o descentralizada de datos biométricos para la identificación o autenticación de pasajeros a fin de agilizar el flujo de pasajeros en los aeropuertos, ni sobre la compatibilidad de dicho tratamiento con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD.

11. Por estas razones, el Comité considera que la solicitud es admisible y que las cuestiones que se derivan de ella deben analizarse en un dictamen adoptado de conformidad con el artículo 64, apartado 2, del RGPD.

2 ÁMBITO DE APLICACIÓN y CONTEXTO DEL DICTAMEN

2.1 Ámbito de aplicación del Dictamen

12. El presente Dictamen se refiere solo a la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD, del uso de la tecnología de reconocimiento facial para la autenticación o identificación de pasajeros mediante datos biométricos por parte de los gestores aeroportuarios y las compañías aéreas, **con el fin específico de agilizar el flujo de pasajeros en los aeropuertos**, concretamente en los controles de seguridad, la entrega de equipajes, el embarque y el acceso a la sala de pasajeros, según la solicitud.

13. En cuanto al **ámbito presente Dictamen**, el Comité aclara lo siguiente:

    1) El tratamiento de datos personales en el marco de los controles fronterizos y de los controles efectuados por las tiendas libres de impuestos no entra en el ámbito del presente Dictamen, ya que es efectuado por responsables del tratamiento distintos de los gestores aeroportuarios y las empresas de transporte aéreo.

    2) El uso de la tecnología de reconocimiento facial, aunque se base en los escenarios descritos más adelante en la sección 3.2, para cualquier otro fin (como la aplicación de la ley) o por cualquier otra parte, aunque sea para fines similares, queda fuera del ámbito del presente Dictamen.

[6] Solicitud, pp. 1 a 3.
[7] Artículo 64, apartado 3, del RGPD y artículo 10, apartado 4, del Reglamento interno del CEPD.
[8] Directrices 3/2019 del CEPD sobre el tratamiento de datos personales mediante dispositivos de vídeo, versión 2.0, adoptadas el 29 de enero de 2020 (en lo sucesivo, las «**Directrices 3/2019 del CEPD sobre dispositivos de vídeo**»).

3) El presente Dictamen solo examina el tratamiento de los datos personales de los pasajeros y no abarca otros tipos de interesados, como el personal de los gestores aeroportuarios o de las compañías aéreas.

4) El presente Dictamen examina la solicitud presentada por la AC FR en relación con la compatibilidad de las arquitecturas de conservación de las plantillas biométricas de los pasajeros con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD. A este respecto, el Dictamen no incluye un análisis completo y exhaustivo sobre el cumplimiento del RGPD por parte del responsable o responsables del tratamiento pertinentes en cada caso, así como de sus encargados del tratamiento, cuando proceda. Esto es especialmente importante teniendo en cuenta que estas tecnologías conllevan mayores riesgos asociados al tratamiento de las categorías especiales de datos de conformidad con el artículo 9 del RGPD. Por lo tanto, el presente Dictamen se entiende sin perjuicio de una evaluación relativa a otras disposiciones del RGPD en lo que respecta al uso de tecnologías de reconocimiento facial, también en el sector específico al que se refiere la solicitud, o de un análisis jurídico y técnico caso por caso en función del tratamiento específico previsto por un responsable del tratamiento y de las circunstancias.

5) El presente Dictamen no examina el tratamiento de los datos personales de los menores y se entiende sin perjuicio de los requisitos específicos aplicables a este respecto.

6) El presente Dictamen se entiende sin perjuicio de los requisitos legales y otras restricciones para el uso de datos biométricos derivados del Derecho nacional de los Estados miembros[9].

7) Cualquier conclusión del presente Dictamen se entiende sin perjuicio de los nuevos avances tecnológicos.

8) El presente Dictamen examina cuatro escenarios, cuyas características específicas se describen a continuación en la sección 3.2. No aborda otros escenarios, aunque el tratamiento se realice con los mismos fines.

14. En su solicitud, la AC FR indicó que el tratamiento de los datos biométricos de los pasajeros con el fin de agilizar el flujo de pasajeros en los aeropuertos se basaría en el supuesto de que las personas dan su consentimiento a dicho tratamiento, lo que posiblemente constituiría la base jurídica en virtud del RGPD[10]. **Sin embargo, el análisis de la base jurídica aplicable no entra en el ámbito de las cuestiones planteadas al CEPD en la Solicitud y, en consecuencia, en el presente Dictamen no se examina la validez del consentimiento para dicho tratamiento, de conformidad con los artículos 6, 7 y 9 del RGPD.**

15. No obstante, el CEPD señala en términos generales que, si los responsables del tratamiento pertinentes se ampararan en esta base jurídica, tendrían que obtener un consentimiento expreso

[9] Por ejemplo, el artículo 9, apartado 4, del RGPD establece que los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos biométricos.
[10] Solicitud, anexo I.

válido[11] de las personas dispuestas a utilizar dichos servicios. Este consentimiento explícito tendría que darse libremente, ser específico e informado[12], y si se cumplen esas condiciones se analizaría caso por caso. Esto significa, entre otras cosas, que:

1) Las personas tendrían que poder retirar fácilmente su consentimiento en cualquier momento y sin sufrir perjuicio alguno[13].

2) Para que el consentimiento se dé libremente, este uso de tecnologías basadas en la biometría solo puede tener lugar de forma voluntaria, ya que las personas deben poder elegir libremente si utilizan o no estos servicios y sin sufrir perjuicio alguno (por ejemplo, retrasos significativamente más largos para los pasajeros que no dan su consentimiento[14]), incentivos, costes o ventajas adicionales a cambio[15].

3) También habría que solicitar el consentimiento explícito de las personas cuyos datos biométricos se traten, aunque no se hayan registrado para que se les identifique o autentique por esos medios. En otras palabras, es esencial que a las personas que no hayan dado su consentimiento explícito al reconocimiento facial para los fines previstos no se les escanee el rostro con cámaras. Esto puede lograrse, por ejemplo, dedicando filas específicas al reconocimiento facial y proporcionando una señalización adecuada y una separación física con los flujos de control no biométricos para permitir una identificación clara de dichas filas.

4) Sin perjuicio de si el consentimiento fuese la base jurídica aplicable a dicho tratamiento, los principios del tratamiento consagrados en el artículo 5 del RGPD con respecto a la necesidad y la proporcionalidad siguen aplicándose incluso cuando las personas hayan dado su consentimiento explícito para el uso de sus datos biométricos[16].

16. La solicitud especifica[17] que los gestores aeroportuarios actuarían como responsables del tratamiento en los controles de seguridad del aeropuerto, mientras que las compañías aéreas serían las responsables del tratamiento en la entrega de equipajes, el embarque y el acceso a la sala de pasajeros. Por lo tanto, el Comité señala que diferentes agentes podrían participar en el tratamiento descrito en la solicitud y no ha evaluado la aplicación de las funciones de corresponsable y encargado

[11] De conformidad con el artículo 4, apartado 14, y el artículo 9, apartado 1, del RGPD, así como con el artículo 9, apartado 2, letra a), del RGPD, queda prohibido el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física, a menos que el interesado haya dado su consentimiento expreso para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el artículo 9, apartado 1, del RGPD no puede ser levantada por el interesado. Véanse también los considerandos 51, 52 y 53 del RGPD.
[12] Artículo 4, apartado 11, y artículo 7, del RGPD.
[13] Artículo 7, apartado 4, y considerando 50 del RGPD.
[14] Por ejemplo, esto podría incluir consideraciones como el diseño de un sistema para evitar crear una presión social sobre los pasajeros que no desean dar su consentimiento, evitando que su elección afecte negativamente a otros pasajeros.
[15] Directrices 5/2020 del CEPD sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, versión 1.1, adoptadas el 4 de mayo de 2020 (en lo sucesivo, las «**Directrices 5/2020 del CEPD sobre el consentimiento**), apartados 46 y 48.
[16] Ídem, apartado 5.
[17] Solicitud, anexo I.

del tratamiento en los escenarios descritos a continuación en la sección 3.2 del presente Dictamen. En cada caso es necesario identificar a los agentes implicados y asignar claramente sus responsabilidades, de modo que se cumplan los requisitos del RGPD[18].

17. Además, el Comité señala que en la actualidad no existe ninguna obligación normativa uniforme en la UE por la que los operadores aeroportuarios y las compañías aéreas deban identificar a los pasajeros y verificar que el nombre que figure en la tarjeta de embarque del pasajero coincida con el nombre que figure en su documento de identidad en todos los puntos de control mencionados[19]. Por lo tanto, cualquier requisito de este tipo está sujeto a las leyes nacionales que pueden variar de un Estado miembro a otro. En algunos Estados miembros, esta verificación puede ser necesaria para algunos puntos de control (por ejemplo, la entrega de equipaje o el embarque), mientras que en otros no se requieren controles de este tipo en la actualidad[20]. La existencia de obligaciones legales para verificar la identidad de los pasajeros tiene un efecto directo en las prácticas de los distintos aeropuertos.

18. Por consiguiente, en estas situaciones, **en las que no se requiere la verificación de la identidad de los pasajeros con un documento de identidad oficial, no debe realizarse ninguna verificación con el uso de la biometría, ya que esto daría lugar a un tratamiento excesivo de datos, puesto que implica el tratamiento de datos adicionales en comparación con la situación actual e iría más allá de lo necesario para los fines pertinentes, infringiendo el principio de minimización de datos establecido en el artículo 5, apartado 1, letra c), del RGPD**. Esta consideración debe tenerse en cuenta en relación con el examen de todos los escenarios descritos en el punto 3.2 del presente Dictamen.

2.2 Nociones clave

19. Para considerarse datos biométricos en el sentido del artículo 4, punto 14, del RGPD[21], el tratamiento de datos sin procesar, como las características físicas, fisiológicas o conductuales de una persona física deben implicar una medición de dichas características, dado que los datos biométricos son el resultado de tales mediciones.[22]

20. Al tomar la imagen de una cara (una fotografía o un vídeo) llamada «**muestra**» biométrica, es posible extraer una representación digital de características distintas de dicha cara (lo que se denomina

[18] En consonancia con el artículo 4, apartados 7 y 8, el artículo 5, apartado 2, y los artículos 24, 26, 28 y 29 del RGPD. Véanse también las Directrices 07/2020 del CEPD, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD, versión 2.1, adoptadas el 7 de julio de 2021.

[19] El Reglamento pertinente a escala de la UE es el Reglamento de Ejecución (UE) 2015/1998 de la Comisión, de 5 de noviembre de 2015, por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea. Sin embargo, este Reglamento no aborda los controles de los documentos de identidad oficiales en los controles aeroportuarios, y los Estados miembros tienen discrecionalidad para regular este aspecto a nivel nacional.

[20] Esto significa que actualmente no se realiza ninguna verificación o solo se verifica la existencia de la tarjeta de embarque. Por ejemplo, en virtud del Protocolo relativo a la exención de los nacionales de Dinamarca, Finlandia, Noruega y Suecia de la obligación de poseer un pasaporte o permiso de residencia mientras residan en un país escandinavo distinto del suyo, de 22 de mayo de 1954, a partir del 1 de julio de 1954, los ciudadanos de Noruega, Dinamarca, Finlandia y Suecia están exentos de la obligación de poseer un pasaporte u otra identificación de viaje cuando viajen entre estos países.

[21] Véanse también los considerandos 51, 52 y 53 del RGPD.

[22] Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 74.

«**plantilla**»)[23]. Además, el Comité recuerda que una «plantilla biométrica es una representación digital de las características únicas que se han extraído de una muestra biométrica y pueden almacenarse en una base de datos biométrica»[24] y que permiten o confirman la identificación única de una persona física. Además, se «supone que esta plantilla es única y específica para cada persona y, en principio, es permanente a lo largo del tiempo»[25]. Normalmente, en un proceso de comparación destinado a identificar o autenticar a una persona a través del reconocimiento facial, se compara una plantilla biométrica entrante con los objetos conservados para verificar una coincidencia o encontrarla en una base de datos[26].

21. La tecnología de reconocimiento facial puede cumplir dos funciones distintas: autenticación[27] e identificación[28]. Aunque las dos funciones son distintas, ambas se refieren al tratamiento de datos biométricos relacionados con una persona física identificada o identificable[29] y, por lo tanto, constituyen un tratamiento de categorías especiales de datos personales en virtud del artículo 9 del RGPD[30].

22. En concreto:

> La **autenticación** tiene por objeto confirmar una declaración biométrica mediante comparación. Se denomina también verificación de uno-a-uno.
>
> La **identificación** tiene por objeto buscar en una base de datos de registro biométrico para devolver identificadores atribuibles a una sola persona. Esto también se denomina identificación «de uno respecto a muchos».

---

[23] Directrices 5/2022, sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley», versión 2.0, adoptadas el 26 de abril de 2023 (en lo sucesivo, las «**Directrices 5/2022 del CEPD, sobre el reconocimiento facial en la aplicación de la ley**»), apartados 7 y 8.

[24] Ídem, apartado 9.

[25] Ídem.

[26] Directrices 5/2022, sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley, apartados 10 y 11; véase también la norma internacional ISO/IEC 2382-37, 2022-03, Disponible en: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [consultado por última vez el 23 de mayo de 2024] (en lo sucesivo «**ISO/IEC 2382-37**»).

[27] El Comité observa que el futuro Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) (aún no publicado en el Diario Oficial) también define en su artículo 3, punto 36, la «verificación biométrica» como «la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente» [véase la Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión] [COM(2021) 0206 – C9-0146/2021 – 2021/0106(COD)].

[28] Ídem, el artículo 3, punto 35, de la Ley de Inteligencia Artificial define la «identificación biométrica» como «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».

[29] ISO/IEC 2382-37.

[30] Artículo 4, punto 14, del RGPD y Directrices 5/2022 del CEPD sobre el reconocimiento facial en la aplicación de la ley, apartado 12.

23. En ambos casos (identificación y autenticación), las técnicas de reconocimiento facial utilizadas se basan en una concordancia estimada entre plantillas: la que se compara y la(s) de referencia. Desde este punto de vista, son técnicas probabilísticas: la comparación deduce una probabilidad mayor o menor de que la persona sea efectivamente la persona que se ha de autenticar o identificar; si esta probabilidad supera un determinado umbral en el sistema, definido por su usuario o su desarrollador, el sistema entenderá que existe una coincidencia[31].

[31] Directrices 5/2022 sobre el reconocimiento facial en la aplicación de la ley, apartado 11. Véase también la norma ISO/IEC 2382-37.

3 SOBRE EL FUNDAMENTO DE LA SOLICITUD

3.1 Observaciones generales

24. En esta sección se analizan las preguntas formuladas en el apartado 4. En este contexto, el Comité analizará, para la pregunta 1, la compatibilidad con el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD, y para la pregunta 2, la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD.

25. A tal fin, el Comité analizará cuatro escenarios diferentes[32], cuyas características específicas se describen a continuación en la sección 3.2.

26. Como observación preliminar, el Comité recuerda que el uso de datos biométricos y, en particular, de la tecnología de reconocimiento facial conlleva riesgos elevados para los derechos y libertades de los interesados. En primer lugar, el tratamiento en cuestión se refiere a los datos biométricos a los que se concede una protección especial en virtud del artículo 9 del RGPD. En particular, los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean «legibles por máquina» y queden sometidas a su uso posterior[33]. Además, el uso de la tecnología de reconocimiento facial puede dar lugar a riesgos asociados a falsos negativos, sesgos y discriminación[34], y el potencial de uso indebido de los datos biométricos podría tener graves consecuencias para las personas, como la usurpación de identidad o la suplantación[35]. También cabe señalar que, cuando el reconocimiento facial se realiza a distancia y sin la participación activa del interesado, las personas físicas podrían ser aún menos conscientes de dicho tratamiento y de los riesgos asociados. Por último, es importante destacar que las características en las que se basan los datos biométricos pueden considerarse generalmente permanentes y deben tratarse como irrevocables, especialmente en el contexto del reconocimiento facial[36].

27. Por lo tanto, teniendo en cuenta lo anterior, antes de utilizar estas tecnologías, aunque se consideraran especialmente eficaces, los responsables del tratamiento deben evaluar el impacto en

---

[32] Los cuatro escenarios analizados por el Comité se basan en casos de uso presentados en el anexo I de la solicitud. La AC FR ha aclarado que los casos de uso presentados en el anexo I de la solicitud son ejemplos de aplicación, pertenecientes a un escenario, utilizados con fines ilustrativos.

[33] *Article 29 Working Party Opinion 3/2012 on developments in biometric technologies adopted on 27 April 2012, WP193* [«Dictamen 3/2012 del Grupo del Artículo 29 sobre la evolución de las tecnologías biométricas WP193», documento en inglés] adoptado el 27 de abril de 2012, (en lo sucesivo, el «**Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 sobre tecnologías biométricas**»), p. 4. Cabe señalar que el presente Dictamen se refiere a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (la «Directiva sobre protección de datos»). El RGPD ha ampliado el ámbito de aplicación de las categorías especiales de datos y, a diferencia de la Directiva sobre protección de datos, el RGPD establece que los datos biométricos son categorías especiales de datos (artículo 9 del RGPD).

[34] *Guidelines on facial recognition, Consultative Committee of Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data* [«Directrices sobre el reconocimiento facial, Comité Consultivo del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal», solo en inglés y francés], junio de 2021, p. 15; también las Directrices 5/2022 del CEPD sobre el reconocimiento facial en la aplicación de la ley, apartado 27.

[35] Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 sobre tecnologías biométricas, p. 29.

[36] Directrices 5/2022 sobre el reconocimiento facial en la aplicación de la ley, apartado 104.

los derechos y libertades fundamentales de los interesados y considerar si unos medios menos intrusivos pueden alcanzar su objetivo legítimo del tratamiento[37].

28. El Comité también recuerda que el derecho a la protección de los datos personales no es un derecho absoluto y debe mantener el equilibrio con otros derechos fundamentales protegidos por la Carta de conformidad con el principio de proporcionalidad[38].

29. El artículo 25, apartado 1, del RGPD hace referencia a «los principios de protección de datos» que se enumeran en el artículo 5 del RGPD[39] y que exige aplicarlos desde el diseño «de forma efectiva»[40]. Esto incluye expresamente el principio de minimización de datos en virtud del artículo 5, apartado 1, letra c), del RGPD[41], que exige que los datos personales sean «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados», lo que refleja el principio de proporcionalidad[42]. Además, el artículo 25, apartado 2, del RGPD especifica la obligación de «minimización de datos por defecto», al establecer que se aplica a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad[43].

30. Sin embargo, el artículo 25 del RGPD no exige que los responsables del tratamiento apliquen medidas técnicas y organizativas específicas, sino que exige que las medidas y garantías elegidas sean específicas del contexto y de los riesgos para los derechos y libertades del interesado que plantea el tratamiento[44]. Del mismo modo, el artículo 32 del RGPD sobre la seguridad del tratamiento exige que

---

[37] Considerando 39 del RGPD. Véanse también las Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 73.

[38] Considerando 4 del RGPD. Véase también a este respecto la sentencia del Tribunal de Justicia de 22 de junio de 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (en lo sucesivo, «C-439/19 Latvijas Republikas Saeima»), apartados 98, 110 y 113. Además, el principio de proporcionalidad, como principio general del Derecho de la Unión, exige que los medios empleados por un acto de la Unión permitan alcanzar el objetivo que este persigue y no vayan más allá de lo que es necesario para alcanzarlo [véase la sentencia del Tribunal de Justicia de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, ECLI:EU:C:2010:662 (en lo sucesivo, «C-92/09 y C-93/09 Volker und Schecke»,), apartado 74 y jurisprudencia citada].

[39] Directrices 4/2019 del CEPD relativas al artículo 25. Protección de datos desde el diseño y por defecto, versión 2.0, adoptadas el 20 de octubre de 2020 (en lo sucesivo, las «**Directrices 4/2019 del CEPD sobre la protección de datos desde el diseño y por defecto**»), apartado 11.

[40] El artículo 25, apartado 1, del RGPD dispone: «Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados». Véanse también las Directrices 4/2019 del CEPD, relativas al artículo 25 (Protección de datos desde el diseño y por defecto), apartado 13.

[41] En consecuencia, el considerando 39 del RGPD establece que los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.

[42] C-439/19, Latvijas Republikas Saeima, apartado 98; sentencia del Tribunal de Justicia de 11 de diciembre de 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064 (en lo sucesivo, «C-708/18, M5A-ScaraA»), apartado 48.

[43] Directrices 4/2019 del CEPD, relativas al artículo 25 (Protección de datos desde el diseño y por defecto), apartado 48.

[44] Directrices 4/2019 del CEPD, relativas al artículo 25 (Protección de datos desde el diseño y por defecto), apartado 14.

los responsables y encargados del tratamiento apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas.

31. Es importante señalar que, aunque los pasajeros dieran su consentimiento explícito para el uso de sus datos biométricos con el fin de agilizar el flujo de pasajeros en los aeropuertos, siguen siendo aplicables y deben respetarse los principios del tratamiento consagrados en el RGPD en relación con la necesidad y la proporcionalidad[45].

32. En cuanto al **principio de necesidad**, el Comité estudiará si el tratamiento propuesto es necesario para alcanzar el objetivo perseguido y si el mismo objetivo puede lograrse con la misma eficacia por otros medios menos intrusivos para los derechos y libertades fundamentales del interesado[46]. En cuanto al **principio de proporcionalidad**, el Comité evaluará si el impacto negativo en los derechos y libertades fundamentales de los interesados es proporcional a cualquier beneficio previsto. Si el beneficio es relativamente menor, entonces dicho impacto podría no ser proporcionado[47].

33. En cualquier caso, aunque el Comité considere que uno de los escenarios analizados a continuación podría cumplir los requisitos del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD, corresponde al responsable del tratamiento en cada caso demostrarlo con elementos de hecho. Dicha demostración debe incluir la consideración de escenarios alternativos.

3.2 Sobre la compatibilidad con el artículo 5, apartado 1, letras e) y f), y con los artículos 25 y 32 del RGPD

3.2.1 Escenario 1: conservación de la plantilla biométrica registrada únicamente en manos de la persona para su autenticación

34. En esta sección se examina la compatibilidad con el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD de la conservación de la plantilla biométrica de los pasajeros únicamente en manos de la persona, por ejemplo, en su dispositivo individual[48], bajo su control exclusivo[49], para su autenticación[50] (en lo sucesivo, el «**escenario 1**»). En esta sección también se examinan las garantías adecuadas para el escenario 1, a la luz de los artículos 25 y 32 del RGPD.

Descripción del escenario

35. En el escenario 1, la plantilla biométrica registrada de cada pasajero que haya dado su consentimiento a dicho tratamiento solo se almacena en su poder, por ejemplo, en un dispositivo individual que lleve

[45] Directrices 5/2020 del CEPD sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, apartado 5.
[46] C-439/19 Latvijas Republikas Saeima, apartados 110 y 113; Sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, apartado 108.
[47] C-708/18 M5A-ScaraA, apartados 52 a 56, C-92/09 y C-93/09 Volker und Schecke, apartado 87; C-439/19 Latvijas Republikas Saeima, apartados 98, 110 y 113. Véase también el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 sobre tecnologías biométricas, p. 8.
[48] Como alternativa, la persona podría imprimir y conservar su plantilla biométrica en papel.
[49] Esto se entiende sin perjuicio de la responsabilidad general del responsable del tratamiento en relación con el tratamiento.
[50] Como ejemplifica el caso de uso 1 del anexo I de la solicitud.

cada pasajero, bajo su control exclusivo. Los pasajeros se autentican (comparación 1:1) cuando pasan por controles específicos en el aeropuerto.

36. El registro lo realiza el gestor del aeropuerto, bien a distancia a través de la aplicación del operador del aeropuerto[51], bien en las terminales del aeropuerto con un nivel adecuado de seguridad de la identidad (por ejemplo, un nivel de seguridad de eIDAS adecuado[52]). Dicho registro consiste en grabar, en el dispositivo del pasajero, una plantilla biométrica y los datos de identificación[53] (en lo sucesivo, los «**datos de identidad**») necesarios para el tratamiento. El registro se produce una sola vez y durante un período de validez específico (por ejemplo, ajustado al período de validez del pasaporte de los pasajeros). El gestor aeroportuario no conserva los datos de identidad ni biométricos de los pasajeros tras el proceso de registro.

37. En particular, en lo que respecta a la conservación, los datos de identidad y la plantilla biométrica del pasajero se almacenan localmente en el dispositivo de cada pasajero (por ejemplo, la aplicación móvil del gestor del aeropuerto o en una aplicación de cartera digital). El dispositivo puede utilizarse para transmitir o consultar los datos de identidad y la plantilla biométrica de los pasajeros, que posiblemente incluyan información sobre el vuelo o la tarjeta de embarque. Por ejemplo, esta información está cifrada con una clave que solo obra en poder del gestor del aeropuerto, quizá codificada en forma de un código QR que puede imprimirse en papel o mostrarse en la pantalla del dispositivo del pasajero. En este caso, el pasajero mostraría entonces este código QR en unidades de control específicas en el aeropuerto, equipados con un escáner QR y una cámara.

38. Desde el punto de vista de la seguridad, durante el cotejo, los códigos QR se descifran con una clave en poder del gestor aeroportuario, que es el único capaz de descifrar los códigos QR. Los datos biométricos de los pasajeros solo se conservan durante un periodo muy breve y se eliminan una vez finalizado el cotejo. Cabe señalar que las medidas de seguridad relativas a la conservación dependen en parte de la seguridad del dispositivo del pasajero.

Evaluación del CEPD

39. El escenario 1 describe las medidas técnicas y organizativas diseñadas para garantizar un nivel de seguridad adecuado a los riesgos para los interesados, tal como se exige en el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD. Los pasajeros se autentican (comparación 1:1) cuando pasan por controles específicos en el aeropuerto. En este escenario, la operación principal de cotejo se realiza

[51] El CEPD señala que podrían contemplarse formas alternativas de registro en el futuro y que dicho registro podría llevarse a cabo sin una aplicación específica del gestor aeroportuario, por ejemplo, mediante la interacción con una cartera digital del usuario.

[52] Un marco para la identificación electrónica y los servicios de confianza (en lo sucesivo, «**eIDAS**») basado en el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital.

[53] A efectos del presente Dictamen, por datos de identificación se entienden datos como los apellidos, el nombre, la fecha de nacimiento, etc., cuya exactitud ha sido verificada en relación con un documento de identidad o un pasaporte.

en el contexto de un entorno controlado[54], en el que los pasajeros participan activamente y tienen más control sobre sus datos. En concreto, solo se controlaría a los pasajeros que dieron su consentimiento para dicho tratamiento y, dado que se les controlaría en unidades específicas, no se recogerían los datos biométricos de otros pasajeros que no hubieran dado su consentimiento para dicho tratamiento. Además, los pasajeros que dan su consentimiento tienen la posibilidad de interrumpir el tratamiento en cualquier momento suprimiendo los datos de su dispositivo.

40. El uso del reconocimiento facial basado en una plantilla biométrica conservada únicamente en manos de la persona, que puede, por ejemplo, estar en un dispositivo individual guardado por el pasajero bajo su control exclusivo, utilizado para la autenticación en controles específicos a través de una interfaz específica, presenta en determinadas condiciones menos riesgos que el uso de datos biométricos cuando los datos se conservan en una base de datos centralizada[55]. Esta conservación localizada, acompañada de garantías adecuadas[56], reduce la gravedad de las violaciones de la seguridad de los datos personales en comparación con la conservación centralizada, en lo que respecta al número de personas afectadas, y garantiza que el acceso a la plantilla biométrica implique una participación activa del interesado.

41. Además, el cotejo podría realizarse localmente en el aeropuerto, comparando la plantilla biométrica, por ejemplo, contenida en el código QR, con el resultado de la plantilla calculada a partir de la muestra biométrica captada por la cámara de la unidad de control. El resultado del cotejo solo lo conocería y utilizaría el responsable del tratamiento que realizara un control específico (que podría ser un gestor aeroportuario o una compañía aérea en función de si se realiza en los controles de seguridad del aeropuerto, la entrega de equipajes, el embarque o el acceso a la sala de pasajeros). Además, el hecho de que la información necesaria para el cotejo (por ejemplo, el código QR) tenga que ser facilitada por la persona actúa como un segundo factor[57] y refuerza así la seguridad de la autenticación.

42. En cuanto a la compatibilidad con el artículo 25 del RGPD y, en particular, con el fin de cumplir el requisito de minimización de datos, debe garantizarse que el tratamiento cumpla el principio de necesidad. En el escenario 1, podría considerarse que las medidas elegidas cumplen el principio de necesidad en relación con la finalidad perseguida (es decir, agilizar el flujo de pasajeros) si, en función de las circunstancias del tratamiento, el responsable de este puede demostrar que no existen soluciones alternativas menos intrusivas que permitan alcanzar el mismo objetivo con la misma eficacia. Por ejemplo, el responsable del tratamiento podría demostrar que, aunque los pasajeros tuvieran que mostrar su dispositivo, el escenario 1 acelera el proceso de verificación en comparación con la situación actual, que incluye que un humano compruebe si el nombre que figura en la tarjeta de embarque coincide con el documento de identidad del pasajero[58]. En particular, esto no podría

[54] «Entorno no controlado» se refiere al uso del reconocimiento facial para la identificación sin la participación activa de los interesados, en el que la plantilla de cada cara que entra en la zona de supervisión se compara con las plantillas de una amplia sección transversal de la población almacenada en una base de datos, véanse las Directrices 5/2022 del CEPD sobre el reconocimiento facial en la aplicación de la ley, apartado 17.

[55] Directrices 5/2022 sobre el reconocimiento facial en la aplicación de la ley, apartado 17.

[56] Como se indica más adelante en el apartado 46.

[57] Por ejemplo, esto reduce el riesgo de suplantación de identidad. Véase también la salvaguardia C.1.2 a continuación.

[58] También podría argumentarse que el control biométrico puede ser menos propenso a errores que un control humano.

demostrarse si actualmente no se realizan controles para verificar la identidad de los pasajeros sobre la base de su documento de identidad oficial (véase, a este respecto, el apartado 18).

43. Además, el gestor aeroportuario no conserva las plantillas biométricas tras el registro y el plazo de conservación de los datos biométricos por parte del responsable del tratamiento que realiza el control es muy breve, ya que dichos datos se eliminan en cuanto finaliza el cotejo. Así pues, las medidas elegidas en el escenario 1 parecen limitar el alcance del tratamiento y el plazo de conservación de los datos personales.

44. En cuanto al principio de proporcionalidad, el carácter intrusivo de dicho tratamiento puede contrarrestarse con la participación activa de los pasajeros, ya que sus datos biométricos se conservarían solo en sus manos. Además, teniendo en cuenta las medidas descritas anteriormente y suponiendo que el responsable del tratamiento aplique las garantías adecuadas que requiera el tratamiento específico en cuestión, la aplicación de las medidas adecuadas podría garantizar un nivel de seguridad adecuado al riesgo. En ese caso, el impacto negativo en los derechos y libertades fundamentales de los interesados podría considerarse proporcional al beneficio previsto.

45. Por lo tanto, teniendo en cuenta lo anterior, en respuesta a la pregunta 1.1, el Comité concluye que dicho tratamiento **podría considerarse, en principio, compatible con el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD, con sujeción a las garantías adecuadas**.

Garantías adecuadas

46. En este tipo de escenario, en respuesta a la pregunta 1.2, el CEPD considera que deben aplicarse al menos las siguientes garantías. Podrían utilizarse otras garantías distintas de las descritas en el presente Dictamen para lograr los mismos objetivos de seguridad y protección de los datos, y podrían ser lícitas siempre que garanticen el cumplimiento del marco jurídico aplicable.

47. Nota: esta es una visión general de alto nivel y no exhaustiva de las posibles garantías apropiadas que debería aplicar un responsable del tratamiento en una solución similar al escenario 1. Su conveniencia con arreglo a los artículos 25 y 32 del RGPD dependerá de un análisis caso por caso. Todos los responsables del tratamiento tendrán que garantizar que llevan a cabo su propia evaluación de impacto relativa a la protección de datos (en lo sucesivo, «EIPD»)[59] y que sus soluciones específicas pueden requerir medidas adicionales no incluidas en el presente Dictamen.

A. Observaciones generales

A.1. Evaluación de impacto relativa a la protección de datos

A.1.1. Realizar una EIPD, de conformidad con los requisitos del artículo 35 del RGPD, siempre que el responsable del tratamiento prevea una nueva operación de tratamiento que implique un tratamiento que pueda dar lugar a un alto riesgo. Es probable que este sea el caso del escenario 1, ya que implica el tratamiento de datos biométricos a gran escala[60]. Evaluar la

[59] Artículo 35 del RGPD.

[60] Artículo 35, apartado 3, del RGPD y Directrices del Grupo de Trabajo del Artículo 29 sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, adoptadas el 13 de octubre de 2017, WP248 rev.01, refrendadas por el CEPD.

conveniencia de implantar un sistema de reconocimiento facial, en particular su necesidad y proporcionalidad con respecto a su finalidad[61], durante la fase inicial de diseño y revisarlo a lo largo de todo el ciclo de vida del desarrollo del producto;

A.1.2. Consultar a la autoridad de control pertinente en caso de que el tratamiento siga generando un alto riesgo a pesar de las medidas adoptadas por el responsable del tratamiento para mitigarlo[62].

A.2. Derechos de los interesados y garantías que pueden aplicar los responsables del tratamiento

A.2.1. Garantías para abordar los casos de falsos negativos. Mitigar el riesgo de sesgo racial, de edad y de género y, para ello, «[s]e evaluará periódicamente si los algoritmos están funcionando en consonancia con los fines y se ajustarán para mitigar sesgos ocultos y garantizar la lealtad del tratamiento»[63]. Por ejemplo, mediante la supervisión e intervención humanas, con el fin de mitigar cualquier sesgo y garantizar que no haya estigmatización ni elaboración de perfiles de pasajeros;

A.2.2. Garantizar que todo tratamiento de datos personales sea transparente y que las personas conozcan y controlen cómo se tratan sus datos para cada operación de tratamiento[64];

A.2.3. Garantizar la aplicación de medidas para cumplir el principio de limitación de la finalidad, de modo que los datos no se utilicen para otros fines, como la seguridad o la formación;

A.2.4. Garantizar que no se capte ninguna foto o vídeo, aunque no se registre ni se trate, de personas que no den su consentimiento al reconocimiento facial mediante medidas adecuadas (como utilizar una profundidad de campo y una zona de captura adecuadas para evitar captar imágenes de otros pasajeros en segundo plano o en los alrededores, desplegar colas específicas claramente etiquetadas para el reconocimiento facial);

A.2.5. Cuando las mismas unidades puedan ser utilizadas por pasajeros que consientan y no consientan el reconocimiento facial, o cuando pasajeros que no consientan el reconocimiento facial puedan aparecer en el campo de visión mientras no se utiliza el sistema, esperar una acción positiva de un pasajero que consienta antes de iniciar la captura de la foto o el vídeo;

[61] Artículo 35, apartado 7, letra b), del RGPD.
[62] Artículo 36, apartado 1, del RGPD.
[63] Directrices 4/2019 del CEPD, relativas al artículo 25 (Protección de datos desde el diseño y por defecto), apartado 70 y nota a pie de página 60.
[64] Directrices 4/2019 del CEPD, relativas al artículo 25 (Protección de datos desde el diseño y por defecto), apartado 68, y considerando 7 del RGPD.

A.2.6. Posibilidad de que un interesado lleve a cabo, en cualquier momento, la supresión de los datos que se encuentran únicamente en sus manos (plantilla biométrica[65]), tal como se conservan en una aplicación móvil o en una cartera digital[66];

A.2.7. Existencia de alternativas viables o soluciones de respaldo (es decir, para los pasajeros que no consientan en la utilización de sus datos biométricos, para los pasajeros que no puedan utilizar dichas soluciones o para los pasajeros que sufran falsos rechazos), a fin de garantizar también que los pasajeros que no den su consentimiento no sufran ningún perjuicio[67];

A.2.8. Si se utiliza una aplicación, debe diseñarse y configurarse cuidadosamente para no recoger datos innecesarios y evitar el uso de kits de desarrollo de *software* de terceros («SDK») que recojan datos para otros fines.

A.3. Responsabilidad proactiva

A.3.1. Evaluar si existen códigos de conducta o mecanismos de certificación pertinentes para ayudar a demostrar el cumplimiento de la seguridad del tratamiento del artículo 32 del RGPD[68]. Verificar la idoneidad de las medidas para el tratamiento concreto de que se trate. Las normas[69], las buenas prácticas y los códigos de conducta reconocidos por las asociaciones y otros organismos que representan a categorías de responsables del tratamiento pueden ser útiles para determinar las medidas adecuadas;

A.3.2. Garantizar que se lleven a cabo controles de seguridad básicos en el dispositivo de los usuarios para permitir la fase de registro, aunque el pasajero también desempeñe un papel en la protección de sus datos, ya que estos se conservan en su dispositivo. En la sección C.2 «Infraestructura y red» se presentan ejemplos de tales comprobaciones y controles técnicos.

B. Aspectos organizativos:

B.1 Política y cumplimiento

B.1.1. Garantizar que se establezcan controles internos de acceso[70] con normas para los administradores;

B.1.2. Cuando el servicio de reconocimiento facial pueda ser prestado por una de las partes implicadas en el tratamiento sin que los datos de identidad o biométricos, o de ambos tipos,

[65] Las referencias a la plantilla biométrica en las garantías para el escenario 1 corresponden a referencias a la clave o código secreto en el escenario 2.
[66] Téngase en cuenta que esta garantía solo se aplica al escenario 1.
[67] Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 86.
[68] Artículo 32, apartado 3, del RGPD y Directrices 4/2019 del CEPD, relativas al artículo 25 (Protección de datos desde el diseño y por defecto), apartado 10.
[69] Véase, por ejemplo, la norma ISO/IEC 2382-37.
[70] Directrices 04/2020 del CEPD sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, adoptadas el 21 de abril de 2020 (en lo sucesivo, «**Directrices 04/2020 del CEPD sobre datos de localización y herramientas de rastreo de contactos**»), SEC-10, p. 16.

tengan que ser tratados por las otras partes implicadas, prohibir que esos datos pasen por esas otras partes. Por ejemplo, una compañía aérea no necesita acceder técnicamente a los datos biométricos cuando se basa en la infraestructura común del aeropuerto, aunque dicha compañía aérea actúe como responsable del tratamiento con arreglo al RGPD;

B.1.3. Definir una política de cifrado y gestión de claves[71], por ejemplo, para el tratamiento de datos de identidad y biométricos;

B.1.4. Garantizar el cumplimiento del capítulo V del RGPD. Por ejemplo, garantizar transferencias conformes si el responsable del tratamiento utiliza un servicio remoto durante el proceso de registro que tiene su sede en un tercer país;

B.1.5. Cuando se utilicen encargados del tratamiento, garantizar que exista un contrato de encargado del tratamiento[72] en consonancia con el artículo 28, apartado 3, del RGPD;

B.1.6. Garantizar la existencia de procedimientos para gestionar la supervisión y la intervención humanas, en particular para tratar los problemas de falsos rechazos y los problemas técnicos o de usabilidad.

B.2. Formación y pruebas

B.2.1. Garantizar que el personal reciba la formación adecuada;

B.2.2. Poner en marcha un «proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento»[73];

B.2.3. Poner en marcha un proceso para garantizar que el tratamiento de la plantilla biométrica del pasajero[74] para la autenticación sea técnicamente eficaz y suficientemente preciso;

B.2.4. Garantizar que las muestras biométricas recogidas tanto en el momento del registro como en el puesto de control sean de calidad suficiente para llevar a cabo un tratamiento biométrico fiable.

C. Aspectos técnicos:

C.1. Acceso

[71] Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 89.
[72] Artículo 28, apartado 3, del RGPD.
[73] Artículo 32, apartado 1, letra d), del RGPD.
[74] Las referencias a la plantilla biométrica en las garantías para el escenario 1 corresponden a referencias a la clave o código secreto en el escenario 2.

C.1.1. Aplicar garantías durante la fase de registro para garantizar el arranque del proceso de inscripción con una identidad verificada. Por ejemplo, para reforzar la evaluación de la identidad de los usuarios se puede aplicar la autenticación multifactorial, desde enlaces protegidos por contraseña de un solo uso para activar la aplicación, hasta mecanismos de desbloqueo de dispositivos locales;

C.1.2. Aplicar garantías para hacer frente a los casos de falsos positivos, ataques de presentación y prevención del fraude[75];

C.1.3. Prohibición de todo acceso externo a los datos de identidad y biométricos[76];

C.1.4. Garantizar que el tratamiento se realiza a nivel local en las fases de registro, transmisión y cotejo. El punto de cotejo debe estar lo más cerca posible del dispositivo de la persona. Habilitar el cotejo de plantillas dentro del dispositivo individual podría requerir la interacción con proveedores de servicios situados fuera del aeropuerto e implicar el uso de recursos de red públicos, con el inconveniente de afectar a la disponibilidad y propagar la plantilla a entidades externas;

C.1.5. Autenticar a un usuario para añadir un nuevo vuelo y generar un nuevo código QR cifrado;

C.1.6. Implantar medidas para hacer frente a la situación en la que un pasajero pueda perder el acceso a su código QR.

C.2. Infraestructura y red

C.2.1. Condiciones sobre el sistema operativo («SO») actualizado y la autenticación habilitada para el acceso al dispositivo para que la aplicación/cartera digital funcione, incluso con la eliminación automática de los datos biométricos y de identificación si el SO está obsoleto y plantea riesgos de seguridad;

C.2.2. Aislamiento de las unidades correspondientes (es decir, los *puntos de control*) de la red cuando estén en funcionamiento y adopción de todas las demás medidas necesarias para garantizar la seguridad;

C.2.3. Realizar la comparación biométrica en el dispositivo del pasajero o en el punto de control (*edge computing*);

[75] *ENISA Report on Digital Identity on leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust* [«Informe de ENISA sobre la identidad digital sobre el aprovechamiento del concepto de identidad autosoberana (SSI) para construir confianza», documento en inglés], de enero de 2022.
[76] Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 89.

C.2.4. Soluciones para abordar las vulnerabilidades de seguridad de los dispositivos individuales de los pasajeros, incluido el cifrado (como mínimo) de datos biométricos y de identidad almacenados;

C.2.5. Utilizar un almacenamiento seguro para (al menos) los datos biométricos únicamente en manos del usuario[77], por ejemplo, mediante un enclave seguro en un teléfono inteligente;

C.2.6. Garantías de seguridad para salvaguardar la seguridad física de las instalaciones, incluida la terminal biométrica del aeropuerto. Garantizar un alto nivel de seguridad para los elementos de la arquitectura que tratan (por ejemplo, computación, flujo de datos, conservación transitoria o a largo plazo) datos de identidad y biométricos.

C.3. Control de identidad del usuario, seguridad y gestión de los datos

C.3.1. Compartimentar los datos durante su transmisión y conservación en al menos tres grupos diferentes, como: datos de identidad, datos biométricos y de vuelo[78]. Garantizar que los datos estén debidamente cifrados entre la transmisión y la conservación;

C.3.2. Implantar medidas técnicas para garantizar que solo se tratan y verifican en el puesto de control los datos que pueden tratarse lícitamente;

C.3.3. Garantizar la eficacia de la supresión de datos[79] mediante un procedimiento seguro de supresión (por ejemplo, memoria principal, caché, posibles copias de seguridad) y evaluar cuándo debe automatizarse la supresión de los datos. Los plazos de conservación de datos deben aplicarse estrictamente mediante rutinas automáticas sin necesidad de una acción complementaria por parte de la persona[80];

C.3.4. Garantizar la autenticidad e integridad de los datos (por ejemplo, firma)[81];

C.3.5. Conservar los datos biométricos de los pasajeros en el punto de registro y en el puesto de control solo durante un plazo muy breve y borrarlos en cuanto el pasajero haya pasado por el puesto de control;

C.3.6. Si se utiliza una aplicación para el registro, aplicar normas de seguridad para la seguridad de las aplicaciones móviles durante el desarrollo de la aplicación, así como pruebas de seguridad por parte de un tercero;

[77] Las referencias a la plantilla biométrica en las garantías para el escenario 1 corresponden a referencias a la clave o código secreto en el escenario 2.
[78] Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 89.
[79] Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 89.
[80] Directrices 4/2019 del CEPD, relativas al artículo 25 (Protección de datos desde el diseño y por defecto), apartado 82.
[81] Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 89.

C.3.7. Garantizar la aplicación de medidas de seguridad durante la fase de registro en el aeropuerto para preservar la confidencialidad y la integridad de los datos biométricos del pasajero. Por ejemplo, si el quiosco imprime el código QR, este no debe mostrarse en el quiosco para evitar que un tercero malintencionado tome una fotografía. En los casos de transmisión de corto alcance, la transmisión debe realizarse sobre la base de la participación activa del usuario y a través de un canal que garantice la proximidad;

C.3.8. Los datos que solo estén a manos de la persona[82] deben conservarse en un lugar seguro en el dispositivo de la persona y cualquier posible vulnerabilidad relacionada con los sistemas operativos del dispositivo debe someterse a los parches de seguridad adecuados. En el caso de un código QR impreso, se debe informar a la persona del carácter especialmente sensible de los datos que contiene y de lo que permite realizar;

C.3.9. Garantizar que el registro se realice siguiendo técnicas adecuadas de prueba de identidad a distancia[83].

3.2.2 Escenario 2: conservación centralizada de la plantilla biométrica registrada de forma encriptada dentro del aeropuerto y con una clave secreta únicamente en manos de los pasajeros, para la autenticación

48. En esta sección se examina la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD de la conservación centralizada, para la autenticación, de las plantillas biométricas de los pasajeros registradas en una base de datos centralizada, de forma cifrada y con una clave o código secreto en poder exclusivo del pasajero[84] (en lo sucesivo, el «**escenario 2**»). En esta sección también se examinan las garantías adecuadas para el escenario 2, a la luz de los artículos 25 y 32 del RGPD.

Descripción del escenario

49. En el escenario 2, el registro se realiza solo una vez, para un periodo de validez determinado (por ejemplo, un año después del último vuelo, hasta la expiración de la validez del pasaporte), ya sea a distancia con el nivel de garantía de la identidad adecuado (por ejemplo, el nivel de garantía adecuado de eIDAS) o en las terminales de los aeropuertos. El registro está controlado por el gestor aeroportuario y consiste en generar datos de identidad y biométricos que se cifran con una clave o código secreto.

50. La base de datos se conserva en las instalaciones del aeropuerto, bajo el control del gestor del aeropuerto. Las claves de cifrado o códigos secretos solo se almacenan en el dispositivo de la persona (por ejemplo, en la aplicación móvil del operador del aeropuerto). La aplicación puede generar un código QR que contiene la clave o código secreto, que puede imprimirse en papel o mostrarse en la

[82] Las referencias a la plantilla biométrica en las garantías para el escenario 1 corresponden a referencias a la clave o código secreto en el escenario 2.
[83] Véase *ENISA Report on Remote ID Proofing: Analysis of methods to carry out identity proofing remotely* [«Informe de ENISA sobre la comprobación de identidad a distancia: Análisis de métodos para realizar la comprobación de identidad a distancia», documento en inglés], marzo de 2021.
[84] Como ejemplifica el caso de uso 2 del anexo I de la solicitud.

pantalla del dispositivo[85]. Además, el gestor aeroportuario[86] lleva a cabo un segundo nivel de cifrado con claves que él controla.

51. Los pasajeros se autentican (comparación 1:1), al pasar por puntos de control específicos en el aeropuerto. Los pasajeros que opten por pasar por los puntos de control biométricos muestran su código QR en una unidad de control específica equipada con un escáner QR y una cámara. El índice de pasajeros se envía a la base de datos para solicitar la plantilla cifrada que se descarga y comprueba localmente en la unidad o el dispositivo del usuario. Solo el responsable del punto de control conoce y utiliza el resultado del cotejo[87].

52. En este escenario, no existen flujos de datos de identidad y biométricos entre aeropuertos, ni interconexión ni interoperabilidad entre las bases de datos centralizadas.

Evaluación del CEPD

53. En el escenario 2, las plantillas biométricas registradas por los pasajeros se conservan de forma centralizada, pero en forma cifrada y con una clave o código secreto que se conserva exclusivamente en manos de los pasajeros. En el escenario 2, los pasajeros se autentican (comparación 1:1).

54. En este escenario, se propone lograr el objetivo de agilizar el flujo de pasajeros (es decir, aumentando la velocidad de los controles) mediante el uso de un sistema centralizado. El CEPD ha señalado anteriormente que dicha solución podría considerarse una alternativa viable a la conservación descentralizada de las plantillas biométricas registradas[88] (como se describe en el escenario 1), si se dan en presencia de necesidades objetivas y con el uso de las garantías adecuadas (véanse las garantías descritas en el apartado 60).

55. Desde el punto de vista de la seguridad, los datos de cada persona se cifran con la clave específica conservada únicamente por la persona y bajo su control exclusivo. Además, el hecho de que la información necesaria para el cotejo (por ejemplo, el código QR) tenga que ser facilitada por la persona que actúa como un segundo factor[89] y refuerza así la seguridad de la autenticación. Además, el gestor aeroportuario lleva a cabo un segundo nivel de cifrado con claves que él controla. En el escenario 2, el índice de la persona se envía a la base de datos central para recuperar los datos biométricos asociados a ella. A continuación, estos datos se envían (cifrados) a un ordenador localizado en el punto de control en el que se descifran para realizar el cotejo y el responsable del punto de control solo conoce y utiliza el resultado del cotejo. Siempre que la clave o el código secreto de la persona se mantenga en el ordenador localizado en el punto de control y que solo se envíe un índice de pasajeros a la base de datos central para recuperar la plantilla biométrica cifrada, tales

[85] La AC FR ha aclarado aún más la posibilidad de que haya otras soluciones técnicas para enviar la información requerida, por ejemplo, utilizando un protocolo de comunicación de corto alcance.
[86] La clave o código secreto (en manos de la persona) está cifrada a su vez con otra clave mantenida por el operador del aeropuerto.
[87] La AC FR aclaró que este plazo de conservación es ilustrativo y puede considerarse aceptable, dado que la clave se conserva en manos de las personas y podría elegirse en la fase de registro. No obstante, cabe señalar que dichos plazos de conservación pueden adaptarse.
[88] Directrices 3/2019 del CEPD sobre dispositivos de vídeo, apartado 88.
[89] Por ejemplo, esto reduce el riesgo de suplantación de identidad. Véase también la garantía C.1.2.

medidas de seguridad podrían considerarse compatibles con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD.

56. En cuanto a la compatibilidad con el artículo 25 del RGPD y, en particular, con el fin de cumplir el requisito de minimización de datos, debe garantizarse que el tratamiento cumpla el principio de necesidad. En el escenario 2, podría considerarse que las medidas elegidas cumplen el principio de necesidad en relación con la finalidad perseguida (es decir, agilizar el flujo de pasajeros en los aeropuertos) si, en función de las circunstancias del tratamiento, el responsable de este puede demostrar que no existen soluciones alternativas menos intrusivas que permitan alcanzar el mismo objetivo con la misma eficacia. En el escenario 2, los pasajeros tendrían que mostrar su dispositivo[90]. No obstante, el responsable podrá demostrar que el escenario 2 acelera el proceso de verificación si se compara con la situación actual, que incluye la comprobación por parte de un humano de si el nombre que figura en la tarjeta de embarque coincide con el documento de identidad del pasajero[91], o si se compara con el escenario 1. En particular, esto no podría demostrarse si actualmente no se realizan controles para verificar la identidad de los pasajeros sobre la base de su documento de identidad oficial (véase, a este respecto, el apartado 18).

57. En cuanto al principio de proporcionalidad, el carácter intrusivo de dicho tratamiento puede contrarrestarse con la participación activa de los pasajeros, que tienen bajo su control exclusivo la clave de sus datos cifrados. Además, parece que los riesgos para la seguridad derivados de la conservación de los datos biométricos de los pasajeros en una base de datos centralizada y con la clave únicamente en manos de los pasajeros pueden mitigarse mediante el uso de las garantías adecuadas (véanse las garantías que se abordan en el apartado 60). Por lo tanto, suponiendo que el responsable del tratamiento aplique las garantías adecuadas exigidas por el tratamiento específico en cuestión, los riesgos para las personas podrían mitigarse y el impacto negativo en los derechos y libertades fundamentales de los interesados podría considerarse proporcional al beneficio previsto. Por supuesto, en cada caso debe garantizarse que solo se traten los datos necesarios para su finalidad y que solo se controle a los pasajeros que hayan dado su consentimiento, por lo que no existe el riesgo de que se recojan datos biométricos de otros pasajeros que no hayan dado su consentimiento.

58. En la solicitud se indica a modo de ejemplo que, en el escenario 2, el plazo de conservación de los datos cifrados en la base de datos podría ser normalmente de un año después del último vuelo realizado por la persona y hasta la expiración de la validez del pasaporte. En la solicitud no se ha facilitado información para justificar un período tan largo sobre la base de razones objetivas, aunque puede suponerse que dicho plazo de conservación está previsto a efectos de comodidad para vuelos futuros. En cuanto al plazo de conservación, para lograr la compatibilidad con el artículo 5, apartado 1, letra e), del RGPD en este escenario, los responsables del tratamiento deben poder justificar por qué es necesario este plazo para ese fin en casos concretos. El Comité recomienda a los responsables del tratamiento que prevean un plazo de conservación lo más breve posible, teniendo en cuenta

[90] La AC FR ha aclarado también otras opciones para presentar una plantilla, por ejemplo, impresa en papel. Además, el CEPD reconoce que en el futuro podría preverse el uso de una tecnología alternativa, por ejemplo, basada en un sistema de comunicación de campo cercano.

[91] También podría argumentarse que el control biométrico puede ser menos propenso a errores que un control humano.

también a los pasajeros que vuelan solo ocasionalmente, y que ofrezcan a los interesados la posibilidad de fijar el plazo de conservación que prefieran.

59. A la luz de estas consideraciones, en respuesta a la pregunta 2.1.1, el Comité concluye que dicho tratamiento **podría considerarse, en principio, compatible con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD, con sujeción a garantías adecuadas**.

Garantías adecuadas

60. En este tipo de escenario, en respuesta a la pregunta 2.1.2, el Comité considera que, **además de las garantías enumeradas en el escenario 1**, deben aplicarse al menos las siguientes garantías. Podrían utilizarse otras garantías distintas de las descritas en el presente dictamen para lograr los mismos objetivos de seguridad y protección de datos, y podrían ser lícitas siempre que garanticen el cumplimiento de los marcos jurídicos aplicables.

61. Nota: *esta es una visión general de alto nivel y no exhaustiva de las posibles garantías apropiadas, que debería aplicar un responsable del tratamiento en una solución similar al escenario 2. Su conveniencia con arreglo a los artículos 25 y 32 del RGPD dependerá de un análisis caso por caso. Todos los responsables del tratamiento tendrán que garantizar que llevan a cabo su propia EIPD y que sus soluciones específicas pueden requerir medidas adicionales no incluidas en el presente Dictamen.*

D. Observaciones generales

D.1. Derechos de los interesados y garantías que pueden aplicar los responsables del tratamiento

D.1.1. Garantizar el control del pasajero sobre los plazos de conservación para todos sus datos. Los plazos de conservación deben limitarse a lo necesario para el fin específico. Debe fijarse un plazo máximo tras un análisis exhaustivo de factores como la validez del documento de identidad. Debe ofrecerse a los interesados la posibilidad de que fijen el plazo de conservación que prefieran, que podría ser más corto que el plazo predeterminado;

D.1.2. Posibilidad de que un interesado solicite, en cualquier momento, la supresión de datos que se encuentren únicamente en sus manos (clave o código secreto), tal como se conservan en una aplicación móvil o en una cartera digital[92];

D.1.3. Garantizar que la localización de la base de datos central permita una supervisión eficaz por parte de la autoridad de control competente.

E. Aspectos organizativos:

E.1. Política y cumplimiento

[92] Téngase en cuenta que esta garantía solo se aplica al escenario 2.

E.1.1. La confianza en el servidor central debe ser limitada. Garantizar que la gestión del servidor central sigue unas normas de gobernanza claramente definidas e incluye todas las medidas necesarias para garantizar su seguridad[93].

F. <u>Aspectos técnicos:</u>

F.1. Acceso

F.1.1. Mantener registros de quién tiene acceso a los datos personales, en particular los datos de identidad y biométricos, y cuándo se accedió a ellos;

F.2. Infraestructura y red

F.2.1. Proteger adecuadamente la base de datos central, incluso contra ataques de disponibilidad;

F.2.2. Garantizar que no haya conexión a internet con la base de datos central, los módulos de registro y las unidades de cotejo. El funcionamiento y el mantenimiento de este sistema (por ejemplo, copias de seguridad, parches, seguimiento, etc.) se llevarán a cabo localmente dentro de las instalaciones del aeropuerto.

F.3. Seguridad y gestión de los datos

F.3.1. Aplicar las técnicas criptográficas más avanzadas para garantizar los intercambios entre la aplicación y el servidor centralizado[94];

F.3.2. Mantener la clave o código secreto en el nivel en el que se utilizará para descifrar (es decir, en el módulo de control) y solo utilizar el índice para recuperar la plantilla biométrica correspondiente registrada en la base de datos central;

F.3.3. Garantizar el intercambio de la clave o código secreto entre el dispositivo de usuario y la unidad protege la comunicación contra cualquier posible escucha o transmisión a terceros;

F.3.4. Indexar la plantilla biométrica cuando se conserva en la base de datos central para permitir la autenticación 1:1 y garantizar que es única y está relacionada con la persona.

[93] Directrices 04/2020 del CEPD sobre datos de localización y herramientas de rastreo de contactos, PRIV-5, p. 17.

[94] Directrices 04/2020 del CEPD sobre datos de localización y herramientas de rastreo de contactos, SEC-4, p. 18; «Entre las técnicas que pueden utilizarse figuran, por ejemplo, las siguientes: cifrado simétrico y asimétrico, funciones *hash*, prueba privada de pertenencia (*private membership test, PMT*), intersección privada de conjuntos (*private set intersection, PSI*), filtros Bloom, recuperación de información privada, cifrado homomórfico».

Asegurarse de que el índice no revela ninguna información de identificación del pasajero y no está correlacionado con la clave de cifrado;

F.3.5. Autenticar y encriptar adecuadamente cualquier transmisión entre la base de datos central y los puntos de control y ponerla en redes aisladas;

F.3.6. Evitar los enlaces bidireccionales entre conjuntos de datos (datos de identidad y biométricos, así como detalles del vuelo) y mantener solo los enlaces unidireccionales relevantes en la base de datos. Por ejemplo, solo los vínculos unidireccionales del índice a los de identidad, del índice a los datos biométricos cifrados y del índice a los datos del vuelo;

F.3.7. Garantizar mecanismos de continuidad de la actividad, por ejemplo, disponiendo de sistemas de conservación de reserva adecuados;

F.3.8. Garantizar que la unidad no conserve registros de las plantillas cifradas o no cifradas.

3.2.3 Conservación centralizada de las plantillas biométricas registradas con fines de identificación

62. En esta sección se examina la compatibilidad con el artículo 5, apartado 1, letras e) y f), y con los artículos 25 y 32 del RGPD de la conservación centralizada, con fines de identificación, de las plantillas biométricas de los pasajeros que se han registrado, cuando dichas plantillas no están cifradas con una clave o código secreto en poder exclusivo de los pasajeros, en dos casos de uso: 1) cuando dichas plantillas se conserven en una base de datos dentro del aeropuerto, bajo el control del gestor del aeropuerto[95] (en lo sucesivo, el «**escenario 3.1**»); y 2) cuando dichas plantillas se conserven en la nube, bajo el control de la compañía aérea[96] (en lo sucesivo, «**escenario 3.2**»).

63. El Comité considera que el uso de datos biométricos con fines de **identificación** en grandes bases de datos centrales interfiere con los derechos fundamentales de los interesados y podría acarrearles graves consecuencias[97]. Además, el uso de datos biométricos también debe examinarse en relación con la finalidad para la que se tratan, a la luz de los principios de necesidad y proporcionalidad[98].

3.2.3.1 Escenario 3.1: Conservación centralizada en una base de datos dentro del aeropuerto, bajo el control del operador del aeropuerto

Descripción del escenario

[95] Como ejemplifica el caso de uso 3A del anexo I de la solicitud.
[96] Como ejemplifica el caso de uso 3B del anexo I de la solicitud.
[97] Por ejemplo, véase el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 sobre tecnologías biométricas, p. 8. Véase también el apartado 26.
[98] Considerando 4 del RGPD. Véase también el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 sobre tecnologías biométricas, p. 8.

64. En el escenario 3.1, la plantilla biométrica registrada por los pasajeros se conserva en una base de datos central en las instalaciones del aeropuerto y bajo el control del operador del aeropuerto en forma cifrada. En particular, los datos de los pasajeros están compartimentados, lo que significa que sus datos de identidad, la plantilla biométrica registrada y la información de vuelo se conservan en tres bases de datos diferentes. Estos datos se cifran con diferentes claves, tanto durante la conservación como mientras se transmiten a los servidores que realizan el cotejo, donde luego son descifrados por el gestor aeroportuario.

65. Los pasajeros deben registrarse para cada vuelo, en un plazo breve antes de su salida (por ejemplo, cuarenta y ocho horas). Dicho registro puede realizarse a distancia o en las terminales aeroportuarias con un nivel adecuado de garantía de identidad (por ejemplo, un nivel de seguridad eIDAS adecuado). Alternativamente, la inscripción puede adoptar la misma forma que la descrita en el escenario 1, en cuyo caso los pasajeros deben trasladar sus datos de sus carteras digitales al sistema aeroportuario en un plazo de cuarenta y ocho horas antes de su salida.

66. También en este caso, los pasajeros se presentan ante una unidad de control específica equipada con una cámara. A continuación, su muestra biométrica se envía a un servidor central del aeropuerto, que intentará cotejar los datos con los de la base de datos biométrica central. De este modo, se puede identificar al pasajero y comprobar si efectivamente está registrado para un vuelo de salida (o para el embarque en caso de control en el embarque). Dependiendo del punto de control, los datos enviados de vuelta al responsable del tratamiento solicitante pueden minimizarse, por ejemplo, como una «respuesta sí/no» o el propio resultado del cotejo, si es necesario. En este caso, solo el resultado de la solicitud se transmite a un responsable del punto de control, que es el que lo utiliza.

67. En particular, en este escenario se identifican los pasajeros (comparación de 1: N), donde *N* es el número de pasajeros previsto en el aeropuerto en un plazo de varios días. Además, el cotejo biométrico solo se realiza cuando cada pasajero se presenta en puntos de control predeterminados del aeropuerto de partida, pero el propio tratamiento de datos se realiza en un servidor central conectado a la base de datos central. El plazo de conservación en este escenario suele ser de cuarenta y ocho horas y los datos se eliminan una vez que el avión ha despegado.

Evaluación del CEPD

68. Como se ha recordado anteriormente, el tratamiento de datos biométricos conlleva mayores riesgos para los derechos y libertades de los interesados[99]. Así pues, cualquier fallo en la seguridad de los datos puede tener consecuencias especialmente graves para los interesados[100]. Los responsables del tratamiento están obligados a mitigar eficazmente esos riesgos. Dado que en este escenario toda la arquitectura está completamente centralizada, los pasajeros pierden el control de sus datos en mayor medida. Además, el riesgo de que los datos terminen siendo tratados para otros fines distintos del control del flujo de pasajeros también podría ser mayor.

[99] Véase el apartado 26.

[100] *Guidelines on facial recognition, Consultative Committee of Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data* [«Directrices sobre el reconocimiento facial, Comité Consultivo del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal», solo en inglés y francés], junio de 2021, p. 22.

69. A la luz del principio y los requisitos en materia de seguridad [artículo 5, apartado 1, letra f), y artículo 32 del RGPD], debe considerarse que la conservación de datos de identidad y biométricos en bases de datos centrales, aunque separadas, puede proporcionar puntos de ataque de gran valor y una violación de la confidencialidad de dicha base de datos puede implicar posteriormente el acceso a todo el conjunto de datos. Como consecuencia de ello, una posible violación de la seguridad de las plantillas de reconocimiento facial y la identificación asociada puede permitir la identificación no autorizada o ilícita de los interesados en otros entornos. También puede, en función de los métodos utilizados para la identificación biométrica, suponer una amenaza para el futuro uso seguro de las plantillas de reconocimiento facial como identificador. En ese caso, los efectos de la infracción no pueden mitigarse, a diferencia del caso de otro tipo de credencial (por ejemplo, identificador de usuario, contraseña) que es posible cambiar[101].

70. Además, la gran cantidad y la elevada calidad de los datos de identidad y biométricos que posee el responsable del tratamiento lo convierten en un objetivo muy valioso para un atacante, lo que conlleva, en términos de riesgo para la seguridad, un mayor nivel de probabilidad. Además, las violaciones de datos podrían tener un mayor impacto ya que, debido a la conservación de los datos en un lugar centralizado, podría ser más fácil para los atacantes acceder a los datos personales relativos a múltiples pasajeros. Por lo tanto, una posible violación podría exponer a un gran número de interesados a riesgos elevados en términos de gravedad, por ejemplo, usurpación de identidad a gran escala, que son extremadamente difíciles de mitigar.

71. Por lo tanto, en lo que respecta a la compatibilidad con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD, las medidas previstas en el escenario 3.1[102], teniendo en cuenta el estado de la técnica, son insuficientes para garantizar un nivel de seguridad adecuado al riesgo. Sobre esta base, el tratamiento con arreglo al escenario 3.1 no cumpliría lo dispuesto en el artículo 5, apartado 1, letra f), y en el artículo 32 del RGPD, si un responsable del tratamiento se limitara a esas medidas.

72. A la luz del principio del artículo 5, apartado 1, letra e), del RGPD, en este escenario, el plazo de conservación de datos biométricos en la base de datos central suele ser de cuarenta y ocho horas. Esta limitación del plazo de conservación parece reducir significativamente los riesgos asociados a las violaciones de la seguridad de los datos personales. No obstante, el plazo de conservación de datos no es un factor decisivo, por sí solo, para la compatibilidad global de dicha arquitectura, ya que los plazos de conservación pueden estar sujetos a cambios por parte de los responsables del tratamiento. En cualquier caso, las medidas propuestas deben cumplir los requisitos de protección de datos desde el diseño y por defecto con arreglo al artículo 25 del RGPD.

73. A diferencia de los escenarios 1 y 2, en los que se autentica a los pasajeros, en el escenario 3.1 se identifican los pasajeros (comparación de 1: N), donde *N* es el número de pasajeros que se esperan en el aeropuerto en un plazo de varios días que han dado su consentimiento al pasar por puntos de control específicos en el aeropuerto. Esto implica la búsqueda de pasajeros en una base de datos central, mediante el tratamiento de cada muestra biométrica capturada para comprobar si coincide con una persona conocida por el sistema. A diferencia del escenario 2, en el escenario 3.1, las claves no se conservan únicamente en manos de los pasajeros. Por consiguiente, en este escenario, los

[101] Véase, a este respecto, el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 sobre tecnologías biométricas, p. 34.
[102] Como se describe en los apartados 64 a 67.

pasajeros tienen un control significativamente menor sobre sus datos biométricos. Por lo tanto, el tratamiento propuesto en el escenario 3.1 no puede ser compatible con los requisitos de protección de datos desde el diseño y por defecto en virtud del artículo 25 del RGPD.

74. A la luz del artículo 25 del RGPD, los responsables del tratamiento deben tener en cuenta los tipos, las categorías y el nivel de detalle de los datos personales necesarios para los fines del tratamiento[103]. Sus opciones de diseño deben tener en cuenta el aumento de los riesgos para los principios de integridad y confidencialidad, minimización de datos y limitación del plazo de conservación cuando se recogen grandes cantidades de datos personales detallados, y compararlos con la reducción de los riesgos cuando se recogen datos acerca de los interesados en menor cantidad o menos detallados. En cualquier caso, la configuración por defecto no debe incluir la recogida de datos personales que no sean necesarios para el fin concreto del tratamiento. En otras palabras, si algunas categorías de datos personales son innecesarias o si no hacen falta datos detallados porque es suficiente utilizar datos menos pormenorizados, no se recogerán datos personales excesivos. En este caso, si otra implementación del tratamiento puede alcanzar el mismo objetivo y está disponible en los términos descritos en el escenario 3.1, no es necesario utilizar la tecnología de reconocimiento facial.

75. En cuanto al artículo 25 del RGPD, un elemento clave de la protección de datos desde el diseño y por defecto es la autonomía del interesado. En particular, los interesados deben tener el máximo grado de autonomía posible para determinar el uso que se haga de sus datos personales, así como el ámbito y las condiciones de dicho uso o tratamiento[104]. En el escenario 1, el interesado tendría autonomía y control en relación con el uso, la divulgación y la supresión de sus plantillas biométricas y, en el escenario 2, el interesado mantendría cierto control sobre la divulgación de su propia plantilla biométrica, ya que su clave de cifrado o código secreto se conservaría en sus manos. Sin embargo, en el escenario 3.1, el interesado depende plenamente de las decisiones del responsable del tratamiento en relación con el tratamiento de sus datos biométricos y, por lo tanto, no tiene ningún control directo sobre el uso de su plantilla biométrica.

76. En lo que respecta a la compatibilidad con el artículo 25 del RGPD, y en particular para cumplir el requisito de minimización de datos, el tratamiento previsto en el escenario 3.1 no puede cumplir el principio de necesidad. El Comité considera que puede lograrse un resultado similar para agilizar el flujo de pasajeros en los aeropuertos de manera menos intrusiva para la privacidad. Por ejemplo, esto puede lograrse sin el uso de datos biométricos (aunque la experiencia del usuario sería diferente, ya que podría llevarle más tiempo mostrar su tarjeta de embarque y, en caso necesario, los documentos de identificación oficiales). Además, otras soluciones, en particular las que se basan en la conservación de los datos biométricos en una cartera local en el dispositivo de la persona o las que requieren el cifrado de los datos con una clave específica almacenada en el dispositivo de la persona, permiten alcanzar los objetivos de una manera menos intrusiva para la privacidad.

77. En cuanto al principio de proporcionalidad, el tratamiento previsto en el escenario 3.1 crearía riesgos para los derechos de los interesados que no se verían mitigados por las medidas previstas, dado el estado de la técnica. El riesgo de un impacto negativo sobre los derechos y libertades fundamentales

[103] Directrices 4/2019 del CEPD sobre la protección de datos desde el diseño y por defecto, apartado 49.
[104] Directrices 4/2019 del CEPD sobre la protección de datos desde el diseño y por defecto, apartado 70. El considerando 7 del RGPD aclara además que las «personas físicas deben tener el control de sus propios datos personales».

de los interesados que podría derivarse de una violación de la seguridad de los datos en una base centralizada de datos biométricos de un gran número de individuos parece superar el beneficio previsto resultante del tratamiento, ya que dicho beneficio es relativamente menor, es decir, un ligero aumento de la comodidad y la rapidez de los controles. Por lo tanto, no puede justificar el elevado intrusismo de esas medidas para los derechos y libertades fundamentales de las personas y el tratamiento previsto en el escenario 3.1 no cumple el principio de proporcionalidad.

78. A la luz de estas consideraciones, en respuesta a la pregunta 2.2.1, el Comité concluye que, cuando el tratamiento se realiza con el propósito específico de agilizar el flujo de pasajeros en los aeropuertos, el tratamiento previsto en el escenario 3.1:

- **no puede ser compatible con el artículo 25 del RGPD;**
- **no sería conforme con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD** si un responsable del tratamiento se limitara a las medidas descritas en el escenario 3.1.

3.2.3.2 Escenario 3.2: conservación centralizada en una nube, bajo el control de la compañía aérea

Descripción del escenario

79. En el escenario 3.2, la plantilla biométrica registrada por los pasajeros se conserva en la nube, bajo el control de la compañía aérea o de su proveedor de servicios en la nube (encargado del tratamiento de datos). En la Solicitud, se especifica que el proveedor de servicios en la nube estaría situado en el EEE[105]. En este caso, los datos de los pasajeros están cifrados, pero se descifran cuando se utilizan (por ejemplo, cuando se realiza la operación de cotejo), y las claves son controladas por la compañía aérea o su encargado del tratamiento en la nube. Los datos biométricos de los pasajeros se utilizan para la identificación de los pasajeros (comparación de 1: N), donde *N* puede alcanzar el número total de clientes de la compañía aérea[106].

80. Al igual que en los escenarios 1, 2 y 3.1, también en este caso los pasajeros tienen que registrarse en primer lugar. Sin embargo, en el escenario 3.2, el registro de los pasajeros se realiza una vez, mientras el cliente tenga una cuenta en la compañía aérea. El registro se realiza en modo remoto con el nivel de seguridad de la identidad adecuado (por ejemplo, el nivel de seguridad eIDAS adecuado) o en las terminales de los aeropuertos. El cotejo biométrico solo se lleva a cabo cuando los pasajeros se presentan en puntos de control predeterminados del aeropuerto, pero el propio tratamiento de datos se realiza en la nube.

81. En el aeropuerto, los pasajeros pasan por unidades de control específicas, equipadas con una cámara. Los datos biométricos de los pasajeros se envían mediante una solicitud a un servidor en la nube de la aerolínea, donde se realiza el cotejo de estos datos con la base de datos central. De este modo, se puede identificar al pasajero y comprobar si efectivamente está registrado para un vuelo de salida (o para el vuelo de embarque en caso de control en el embarque).

[105] La AC FR aclaró que esto es ilustrativo y que también podrían preverse proveedores de servicios en la nube que no estén situados en el EEE. Además, también podrían contemplarse otras soluciones de conservación (por ejemplo, sin el uso de nubes).
[106] La AC FR aclaró que esto es ilustrativo y que existe una solución en la que los datos biométricos se introducen cada vez antes del vuelo.

82. Potencialmente, los resultados del cotejo pueden ponerse a disposición de múltiples gestores aeroportuarios cuando una compañía aérea disponga de una terminal exclusiva o de acceso a la infraestructura del sistema de información común de un aeropuerto. Dependiendo del punto de control, los datos enviados de vuelta al responsable del tratamiento solicitante pueden minimizarse, por ejemplo, como una «respuesta sí/no» o el propio resultado del cotejo, si es necesario. En este caso, el responsable del tratamiento solo conoce y utiliza el resultado de la solicitud.

83. El plazo de conservación de la plantilla lo define la compañía aérea y puede durar mientras el cliente tenga una cuenta en dicha compañía.

Evaluación del CEPD

84. Las consideraciones ya expresadas por el Comité en relación con el escenario 3.1[107] también se aplican a este escenario.

85. En cuanto al principio y los requisitos en materia de seguridad [artículo 5, apartado 1, letra f) y artículo 32 del RGPD], el tratamiento en el escenario 3.2 se lleva a cabo en la nube y múltiples entidades podrían tener acceso a dichos datos, incluidos posiblemente proveedores no pertenecientes al EEE, incluso cuando los datos se conserven en el EEE[108]. Esta arquitectura entraña riesgos potenciales en relación con las transferencias de datos personales a terceros países. Además, aunque los datos de los pasajeros están cifrados, se descifran cuando se utilizan (por ejemplo, cuando se realiza la operación de cotejo), mientras que las claves son controladas por la compañía aérea o su encargado de tratamiento en la nube. Esta conservación puede dar lugar a un nuevo aumento de la superficie de exposición de seguridad.

86. Por lo tanto, en lo que respecta a la compatibilidad con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD, las medidas previstas en el escenario 3.2[109], teniendo en cuenta el estado de la técnica, son insuficientes para garantizar un nivel de seguridad adecuado al riesgo. Sobre esta base, el tratamiento con arreglo al escenario 3.2 no cumpliría lo dispuesto en el artículo 5, apartado 1, letra f), y en el artículo 32 del RGPD, si un responsable del tratamiento se limitara a esas medidas.

87. Además, según el escenario 3.2[110], los datos podrían conservarse durante un período significativo (es decir, que podría durar tanto tiempo como el interesado tenga una cuenta en la compañía aérea). Esta duración de la conservación expone a los datos a mayores riesgos de violación de su confidencialidad e integridad y parece ir más allá de lo estrictamente necesario y proporcionado para los fines del tratamiento. El Comité señala que el plazo de conservación de los datos no es un factor decisivo, por sí solo, para la compatibilidad global con el RGPD de dicha arquitectura, ya que puede estar sujeto a cambios por parte de los responsables del tratamiento. Sin embargo, sobre la base de la información de que dispone el Comité y que figura en la descripción del escenario 3.2, no existe una justificación suficiente para este largo plazo de conservación ni ninguna medida aparente para mitigar los riesgos para las personas. Sobre esta base, el plazo de conservación propuesto no se limitaría a lo necesario,

[107] Apartado 68 a 77.
[108] *EDPB 2022 Coordinated Enforcement Action on the use of cloud-based services by the public sector* [«Acción de aplicación coordinada del CEPD 2022 sobre el uso de servicios basados en la nube por parte del sector público», documento en inglés], de 17 de enero de 2023, p. 19.
[109] Véase los apartados 79 a 83.
[110] Véase el apartado 83.

de conformidad con el principio de limitación del plazo de conservación del artículo 5, apartado 1, letra e), del RGPD.

88. En cualquier caso, las medidas propuestas en el escenario 3.2 no pueden satisfacer los requisitos de protección de datos desde el diseño y por defecto en virtud del artículo 25 del RGPD. En el escenario 3.2, las plantillas biométricas registradas por los pasajeros se conservan en la nube, bajo el control de la compañía aérea o de su proveedor de servicios en la nube (encargado del tratamiento de datos). Como se ha descrito anteriormente, varias entidades podrían tener acceso a estos datos. Además, los datos biométricos de los pasajeros se utilizan para la identificación de los pasajeros (comparación de 1: N), donde *N* puede alcanzar el número total de clientes/usuarios de la compañía aérea. Dicho método consiste en encontrar a una persona entre un grupo de individuos de la base de datos central, tratando cada rostro capturado para comprobar si coincide con una persona conocida por el sistema. A diferencia del escenario 3.1, en el escenario 3.2 el cotejo podría realizarse a una escala mucho mayor, ya que el criterio aquí es el número de clientes totales de la compañía aérea, mientras que el escenario 3.1 solo incluía el número de pasajeros esperados en un período de varios días.

89. Además, en lo que respecta a la compatibilidad con el artículo 25 del RGPD, y en particular para cumplir el requisito de minimización de datos, el tratamiento previsto en el escenario 3.2 no puede cumplir el principio de necesidad. El Comité considera que un resultado similar de agilización del flujo de pasajeros en los aeropuertos podría lograrse mediante otras medidas menos intrusivas, por ejemplo, sin el uso de datos biométricos, aunque la experiencia del usuario sería diferente, ya que podría llevarle más tiempo mostrar su identificación y su tarjeta de embarque. Además, otras soluciones, en particular las que se basan en la conservación de los datos biométricos en un monedero local en el dispositivo de la persona o las que requieren el cifrado de los datos con una clave específica almacenada en el dispositivo de la persona, permiten al responsable del tratamiento alcanzar los objetivos de una manera menos intrusiva para la privacidad.

90. En cuanto al principio de proporcionalidad, el tratamiento previsto en el escenario 3.2 crearía riesgos para los derechos de los interesados que no se verían mitigados por las garantías previstas. El impacto negativo sobre los derechos y libertades fundamentales de los interesados que se derivaría de una violación de la seguridad de los datos en una base centralizada de datos biométricos de un gran número de individuos conservados en la nube parece superar el beneficio previsto resultante del tratamiento, ya que dicho beneficio es relativamente menor, es decir, un ligero aumento de la comodidad y la rapidez de los controles. Por lo tanto, no puede justificar el elevado intrusismo de esas medidas para los derechos y libertades fundamentales de las personas y el tratamiento previsto en el escenario 3.2 no puede considerarse proporcionado.

91. A la luz de estas consideraciones, en respuesta a la pregunta 2.3.1, el Comité concluye que, cuando el tratamiento se realiza con el propósito específico de agilizar el flujo de pasajeros en los aeropuertos, el tratamiento previsto en el escenario 3.2:

- **no puede ser compatible con el artículo 25 del RGPD;**
- **no sería conforme con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD** si un responsable del tratamiento se limitara a las medidas descritas en el escenario 3.2;
- **no cumpliría lo dispuesto en el artículo 5, apartado 1, letra e), del RGPD**, ya que no existe una justificación suficiente para el plazo de conservación previsto en el escenario 3.2, sobre la base de la información de que dispone el Comité. A fin de cumplir el principio de limitación del plazo de conservación del artículo 5, apartado 1, letra e), del RGPD, el responsable del tratamiento tendría que demostrar que los datos

personales no se conservan más tiempo del necesario para los fines para los que son tratados.

4 CONCLUSIONES

92. En cuanto a la pregunta 1.1, sobre la base de la solicitud de dictamen de la AC FR, en relación con los requisitos del artículo 5, apartado 1, letra f), y de los artículos 25 y 32 del RGPD, y sobre la base del análisis anterior, el Comité concluye que:

93. el uso de la tecnología de reconocimiento facial para la autenticación basada en datos biométricos, con el fin específico de agilizar el flujo de pasajeros en los aeropuertos (controles de seguridad, entrega de equipaje, embarque y acceso a la sala de pasajeros), podría considerarse en principio compatible con los principios de integridad y confidencialidad de conformidad con el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD, en el caso de una arquitectura de conservación en la que la plantilla biométrica registrada de cada pasajero se conserva localmente en su dispositivo individual y bajo su control exclusivo, si está sujeta a las garantías adecuadas descritas en el apartado 46.

94. En cuanto a la pregunta 2.1.1, sobre la base de la solicitud de dictamen de la AC FR, en relación con los requisitos del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD, y sobre la base del análisis anterior, el Comité concluye que:

95. el uso de la tecnología de reconocimiento facial para la autenticación basada en datos biométricos, con el fin específico de agilizar el flujo de pasajeros en los aeropuertos (controles de seguridad, entrega de equipaje, embarque y acceso a la sala de pasajeros), podría considerarse compatible, en principio, con el principio de limitación del plazo de conservación previsto en el artículo 5, apartado 1, letra e), y con los principios de integridad y confidencialidad previstos en el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD, en el caso de una arquitectura de conservación centralizada en la que la plantilla biométrica registrada de cada pasajero se conserva en una base de datos central dentro del aeropuerto, bajo el control del gestor aeroportuario, de forma cifrada, con una clave o código secreto en manos únicamente del interesado, si está sujeta a las garantías adecuadas descritas en el apartado 60.

96. En cuanto a la pregunta 2.2.1, sobre la base de la solicitud de dictamen de la AC FR, en relación con los requisitos del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD, y sobre la base del análisis anterior, el Comité concluye que:

97. el uso de la tecnología de reconocimiento facial para la identificación mediante datos biométricos, utilizada con el fin específico de agilizar el flujo de pasajeros en los aeropuertos (controles de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros) en el caso de una arquitectura de conservación centralizada, cuando las plantillas biométricas registradas de los pasajeros no están encriptadas con una clave o código secreto en manos únicamente de cada pasajero, cuando dichas plantillas se conservan en una base de datos dentro del aeropuerto (bajo el control del operador aeroportuario), no puede ser compatible con el artículo 25 del RGPD. Además, dicho tratamiento no cumpliría el principio de integridad y confidencialidad establecido en el artículo 5, apartado 1, letra f), y en el artículo 32 del RGPD, si un responsable del tratamiento se limitara a las medidas descritas en el escenario 3.1.

98. En cuanto a la pregunta 2.3.1, sobre la base de la solicitud de dictamen de la AC FR, en relación con los requisitos del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD, y sobre la base del análisis anterior, el Comité concluye que:

99. el uso de la tecnología de reconocimiento facial para la identificación mediante datos biométricos, utilizada con el fin específico de agilizar el flujo de pasajeros en los aeropuertos (controles de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros) en el caso de una arquitectura de conservación centralizada, cuando las plantillas biométricas registradas de los pasajeros no están cifradas con una clave/código secreto en manos únicamente de cada pasajero, cuando dichas plantillas se conservan en la nube (bajo el control de la compañía aérea) no puede ser compatible con el artículo 25 del RGPD. Además, dicho tratamiento no cumpliría los principios de integridad y confidencialidad establecido en el artículo 5, apartado 1, letra f), y en el artículo 32 del RGPD, si un responsable del tratamiento se limitara a las medidas descritas en el escenario 3.2. Por último, sobre la base de la descripción del escenario 3.2 y de la información de que dispone el Comité, el tratamiento no cumpliría el principio de limitación del plazo de conservación en virtud del artículo 5, apartado 1, letra e), del RGPD.

Por el Comité Europeo de Protección de Datos

La Presidenta.

(Anu Talus)