Translations proofread by EDPB Members.

This language version has not yet been proofread.

Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley

Versión 2.0

Adoptada el 26 de abril de 2023

Historial de versiones

Versión 1.0	12 de mayo de 2022	Adopción de las directrices para consulta pública
Versión 2.0	26 de abril de 2023	Adopción de las directrices tras la consulta pública

Índice

RESUMEN EJECUTIVO

Cada vez son más las fuerzas y cuerpos de seguridad (FCS) que aplican o tienen intención de aplicar la tecnología de reconocimiento facial (TRF). Puede utilizarse para **autenticar** o para **identificar** a una persona y puede aplicarse a vídeos (por ejemplo, CCTV) o fotografías. Puede utilizarse para diversos fines, como la búsqueda de personas en las listas de observación de la policía o el seguimiento de los movimientos de una persona en el espacio público.

La TRF se basa en el tratamiento de **datos biométricos**, por lo que implica el tratamiento de categorías especiales de datos personales. A menudo, la TRF utiliza componentes de **inteligencia artificial** o aprendizaje automático. Si bien esto permite el tratamiento de datos a gran escala, también genera un riesgo de discriminación y de resultados erróneos. La TRF puede utilizarse en situaciones de control individual, pero también en grandes aglomeraciones y en importantes nodos de transporte.

Es una **herramienta sensible para las FCS.** Las FCS son autoridades ejecutivas y tienen competencias de poder público. La TRF tiende a interferir con los derechos fundamentales (aparte del derecho a la protección de los datos personales) y puede afectar a nuestra estabilidad política social y democrática.

Para la protección de datos personales en el contexto de la aplicación de la ley, deben cumplirse los **requisitos de la Directiva sobre protección de datos en el ámbito penal (DAP)**. La DAP contiene algunas normas relativas al el uso de la TRF; en particular, el artículo 3, punto 13, de la DAP (concepto de «datos biométricos»), el artículo 4 (principios relativos al tratamiento de datos personales), el artículo 8 (licitud del tratamiento), el artículo 10 (tratamiento de categorías especiales de datos personales) y el artículo 11 (mecanismo de decisión individual automatizado).

También otros derechos fundamentales pueden verse afectados por la aplicación de la TRF. Por este motivo, la **Carta de los Derechos Fundamentales de la UE** (en lo sucesivo, «la Carta») es esencial para la interpretación de la DAP, en particular el derecho a la protección de los datos personales establecido en su artículo 8, pero también el derecho a la intimidad consagrado en su artículo 7.

Las medidas legislativas que sirven de base jurídica para el tratamiento de datos personales interfieren directamente en los derechos garantizados por los artículos 7 y 8 de la Carta. El tratamiento de datos biométricos constituye en sí mismo una grave injerencia en cualquier circunstancia y con independencia del resultado (por ejemplo, de una coincidencia encontrada). Toda limitación del ejercicio de los derechos y libertades fundamentales debe estar prevista por la ley y respetar la esencia de dichos derechos y libertades.

La base jurídica debe ser **suficientemente clara** en sus términos para proporcionar a los ciudadanos una indicación adecuada de las condiciones y circunstancias en las que las autoridades están facultadas para recurrir a cualquier medida de recogida de datos y vigilancia secreta. La mera transposición al Derecho interno de la cláusula general que contiene el artículo 10 de la DAP carecería de la necesaria precisión y previsibilidad.

Antes de que el legislador nacional cree una nueva base jurídica para cualquier forma de tratamiento de datos biométricos utilizando el reconocimiento facial, debe **consultarse** a la autoridad de control de la protección de datos competente.

Las medidas legislativas deben ser **adecuadas** para alcanzar los objetivos legítimos perseguidos por la legislación en cuestión. Un **objetivo de interés general**, por muy fundamental que sea, no justifica, por sí mismo, una limitación de un derecho fundamental. Las medidas legislativas deben **diferenciar** y dirigirse a las personas afectadas en función de su objetivo; por ejemplo, la lucha contra delitos graves

específicos. Si una medida abarca a todas las personas de manera general sin tal diferenciación, limitación o excepción, la interferencia se intensifica. Lo mismo sucede si el tratamiento de datos afecta a una parte significativa de la población.

Los datos deben tratarse de manera que se garantice la aplicabilidad y la eficacia de las normas y los principios de protección de datos de la UE. Atendiendo a cada situación concreta, la **evaluación de la necesidad y la proporcionalidad** también debe identificar y tener en cuenta los posibles efectos en otros derechos fundamentales. Si los datos se tratan sistemáticamente sin el conocimiento de los interesados, es probable que se genere una **sensación general de vigilancia constante.** Esto puede dar lugar a efectos disuasorios en relación con algunos o todos los derechos fundamentales afectados, como la dignidad humana en virtud del artículo 1 de la Carta, la libertad de pensamiento, de conciencia y de religión en virtud del artículo 10 de la Carta, la libertad de expresión en virtud del artículo 11 de la Carta y la libertad de reunión y de asociación en virtud del artículo 12 de la Carta.

El tratamiento de categorías especiales de datos, como los datos biométricos, solo puede considerarse «**estrictamente necesario**» (artículo 10 de la DAP) si la injerencia en la protección de los datos personales y sus restricciones se limitan a lo absolutamente necesario, es decir, indispensable, y excluyen todo tratamiento de carácter general o sistemático.

El hecho de que una fotografía haya sido **hecha manifiestamente pública** (artículo 10 de la DAP) por el interesado no significa que los correspondientes datos biométricos que puedan obtenerse de la fotografía por medios técnicos específicos se deban considerar hechos manifiestamente públicos. Los parámetros predeterminados de un servicio, como por ejemplo las plantillas puestas a disposición del público, o la ausencia de elección, como por ejemplo las plantillas hechas públicas sin que el usuario pueda cambiar su configuración, nunca pueden interpretarse como datos hechos manifiestamente públicos.

El artículo 11 de la DAP establece un régimen para los **mecanismos de decisión individual automatizados**. El uso de la TRF implica la utilización de categorías especiales de datos y puede dar lugar a la elaboración de perfiles, dependiendo de la forma y la finalidad para la que se aplique la TRF. En cualquier caso, de conformidad con el Derecho de la Unión y el artículo 11, apartado 3, de la DAP, está prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales.

El artículo 6 de la DAP se refiere a la necesidad de **distinguir entre las diferentes categorías de interesados.** En lo que se refiere a los interesados respecto de los cuales no existen pruebas que puedan sugerir que su conducta podría tener un vínculo, aunque sea indirecto o remoto, con la finalidad legítima según la DAP, lo más probable es que no esté justificada una injerencia.

El **principio de minimización de datos** [artículo 4, apartado 1, letra e), de la DAP] también exige que todo material de vídeo que no sea pertinente para la finalidad del tratamiento sea siempre eliminado o anonimizado (por ejemplo, difuminando sin posibilidad retroactiva de recuperar los datos) antes de su utilización.

El responsable del tratamiento debe estudiar detenidamente si puede cumplir (y cómo) los requisitos relativos a los **derechos del interesado** antes de iniciar cualquier tratamiento de TRF, ya que este implica a menudo el tratamiento de categorías especiales de datos personales sin ninguna interacción clara con el interesado.

El ejercicio efectivo de los derechos del interesado depende de que el responsable del tratamiento cumpla con sus **obligaciones de información** (artículo 13 de la DAP). Para valorar si se da un «caso

concreto» a efectos del artículo 13, apartado 2, de la DAP, hay que tener en cuenta varios factores, entre ellos si los datos personales se han recogido sin el conocimiento del interesado, ya que sería la única forma de permitir a los interesados ejercer efectivamente sus derechos. En caso de que la toma de decisiones se base únicamente en la TRF, los interesados deben ser informados sobre las características de la toma de decisiones automatizada.

Por lo que se refiere a las **solicitudes de acceso,** cuando los datos biométricos se almacenan y se vinculan a una identidad también mediante datos alfanuméricos, en consonancia con el principio de minimización de datos esto debe permitir a la autoridad competente estimar las solicitudes de acceso basada en una búsqueda por esos datos alfanuméricos y sin poner en marcha ningún otro tratamiento de datos biométricos de otras personas (es decir, buscando con TRF en una base de datos).

Los riesgos para los interesados son especialmente graves si se almacenan datos inexactos en una base de datos policial y/o se comparten con otras entidades. El responsable del tratamiento debe **rectificar** los datos almacenados y los sistemas TRF en consecuencia (véase también el considerando 47 de la DAP).

El derecho a la **restricción** adquiere especial importancia cuando se trata de la tecnología de reconocimiento facial (basada en algoritmos y que, por tanto, nunca ofrece un resultado definitivo) en situaciones en las que se recopilan grandes cantidades de datos y pueden variar la precisión y la calidad de la identificación.

Antes de utilizar la TRF es obligatorio realizar una **evaluación de impacto relativa a la protección de datos (véase el artículo 27 de la DAP)**. El CEPD recomienda hacer públicos los resultados de dichas evaluaciones, o al menos las principales constataciones y conclusiones de la evaluación de impacto, como medida de fomento de la confianza y la transparencia.

La mayoría de los casos de utilización de la TRF entrañan un elevado riesgo intrínseco para los derechos y libertades de los interesados. Por consiguiente, la autoridad que despliega la TRF debe **consultar** a la autoridad de control competente antes de implantar el sistema.

Dada la naturaleza única de los datos biométricos, la autoridad que aplique y/o utilice la TRF debe prestar especial atención a la **seguridad del tratamiento,** en consonancia con el artículo 29 de la DAP. En particular, las fuerzas y cuerpos de seguridad deben velar por que el sistema cumpla las normas pertinentes y aplique medidas de protección para las plantillas biométricas. Los principios y garantías de protección de datos deben integrarse en la tecnología antes de iniciarse el tratamiento de datos personales. Por lo tanto, incluso cuando una FCS tenga la intención de aplicar y utilizar TRF de proveedores externos, debe garantizar (por ejemplo, en el procedimiento de contratación) que solo se implanten TRF basadas en los principios de **protección de datos desde el diseño y por defecto**.

El **registro de operaciones** (véase el artículo 25 de la DAP) es una importante garantía para la verificación de la licitud del tratamiento, tanto en el ámbito interno (es decir, el autocontrol del responsable/encargado del tratamiento) como por parte de las autoridades de control externas. En relación con los sistemas de reconocimiento facial se recomienda registrar también los cambios de la base de datos de referencia y los intentos de identificación o verificación, en particular el usuario, el resultado y el grado de certeza. Sin embargo, el registro de operaciones no es sino un elemento esencial del **principio general de rendición de cuentas** (véase el artículo 4, apartado 4, de la DAP). El responsable del tratamiento debe ser capaz de demostrar la conformidad del tratamiento con los principios básicos de protección de datos del artículo 4, apartados 1 a 3, de la DAP.

El CEPD recuerda su petición, formulada conjuntamente con el SEPD, de **prohibición** de determinados tipos de tratamiento en relación con: 1) la identificación biométrica remota de personas en espacios de acceso público; 2) los sistemas de reconocimiento facial basados en la IA que clasifiquen a las personas en grupos, en función de su biometría, por su origen étnico, sexo, orientación política o sexual u otros motivos de discriminación; 3) el uso del reconocimiento facial o tecnologías similares para inferir emociones de una persona física, y 4) el tratamiento de datos personales en un contexto policial partiendo de una base de datos nutrida con datos personales recogidos de forma masiva e indiscriminada, por ejemplo, mediante el «arrastre» *(scraping)* de fotografías e imágenes faciales accesibles en línea.

Una garantía esencial de los derechos fundamentales afectados es la **supervisión efectiva** por parte de las autoridades de control encargadas de la protección de datos. Por lo tanto, los Estados miembros tienen que garantizar que los recursos de las autoridades de control sean adecuados y suficientes para permitirles cumplir sus funciones.

Estas **directrices se dirigen** a los legisladores a escala nacional y de la UE, así como a las FCS y sus agentes que aplican y utilizan los sistemas de TRF. Asimismo, se dirigen a las personas físicas en la medida en que se vean afectadas con carácter general o como interesados, en particular en lo que se refiere a los derechos de los interesados.

Con las **directrices se pretende** informar sobre ciertas propiedades de la TRF y la normativa aplicable en el contexto de observancia de la ley (en particular, la DAP).

- Además, proporcionan una **herramienta para facilitar una primera clasificación de la sensibilidad de un caso determinado** (anexo I).
- También contienen **orientaciones prácticas para las FCS que deseen adquirir y aplicar un sistema de TRF** (anexo II).
- Asimismo, describen varios **casos de uso típicos y enumeran una serie de consideraciones pertinentes**, especialmente en relación con la prueba de necesidad y proporcionalidad (anexo III).

1 INTRODUCCIÓN

1. La tecnología de reconocimiento facial (TRF) puede utilizarse para reconocer automáticamente a las personas por su rostro. A menudo se basa en la inteligencia artificial, como las tecnologías de aprendizaje automático. Las aplicaciones de la TRF se prueban y utilizan en ámbitos cada vez más diversos, desde el uso particular hasta el de las organizaciones privadas y la administración pública. Las fuerzas y cuerpos de seguridad (FCS) también esperan poder hacer un uso provechoso de la TRF, dado que promete soluciones a problemas relativamente nuevos, como las investigaciones que implican una gran cantidad de pruebas, pero también a problemas de siempre, en particular en lo que respecta a la escasez de personal para las tareas de observación y búsqueda.

2. Gran parte del creciente interés por la TRF se basa en su eficiencia y adaptabilidad. Pero también entraña los inconvenientes propios de la tecnología y de su aplicación, especialmente a gran escala. Al ser posible analizar miles de conjuntos de datos personales con solo pulsar un botón, los más leves efectos de discriminación algorítmica o de identificación errónea pueden afectar gravemente a un elevado número de personas en su conducta y en su vida cotidiana. La propia magnitud del tratamiento de los datos personales, y en particular los datos biométricos, es otro elemento clave de la TRF, ya que el tratamiento de datos personales constituye una injerencia en el derecho fundamental a la protección de los datos personales de conformidad con el artículo 8 de la Carta.

3. La aplicación de la TRF por las FCS tendrá (y en cierta medida ya tiene) efectos significativos en las personas individuales y en los grupos, incluidas las minorías, así como implicaciones considerables en nuestra convivencia y en nuestra estabilidad política social y democrática, que concede gran importancia al pluralismo y la discrepancia política. El derecho a la protección de los datos personales suele ser una condición previa esencial para garantizar otros derechos fundamentales. La aplicación de la TRF es muy propensa a interferir en los derechos fundamentales, aparte del derecho a la protección de los datos personales.

4. Por este motivo, el CEPD considera importante contribuir a la actual integración de la TRF en el área de aplicación de la ley cubierta por la Directiva de protección de datos en el ámbito penal[1] y las leyes nacionales que la transponen, y emitir las presentes directrices, con las que se pretenden proporcionar información pertinente a los legisladores a escala nacional y de la UE, así como a las FCS y a sus funcionarios, a la hora de aplicar y utilizar los sistemas de TRF. El ámbito de aplicación de estas directrices se limita a la TRF. Sin embargo, otras formas de tratamiento de datos personales basadas en datos biométricos por parte de las FCS, especialmente si se efectúan a distancia, pueden entrañar riesgos similares o adicionales para las personas, los grupos y la sociedad. En función de las circunstancias, algunos aspectos de estas directrices también pueden ser de utilidad en dichos casos. Por último, también pueden encontrar aquí información importante las personas afectadas con carácter general o en calidad de interesados, en particular por lo que respecta a los derechos de los interesados.

5. Las directrices constan de un documento principal y tres anexos. El documento principal presenta la tecnología y el marco jurídico aplicable. El anexo I contiene una plantilla que ayuda a identificar algunos de los principales aspectos a la hora de clasificar la gravedad de la injerencia en los derechos fundamentales en un ámbito de aplicación determinado. Las FCS que deseen adquirir y gestionar un sistema de TRF pueden encontrar orientaciones prácticas en el anexo II. Dependiendo del ámbito de aplicación de la TRF, pueden ser pertinentes diferentes consideraciones. El anexo III expone una serie de escenarios hipotéticos y las consideraciones pertinentes.

2 TECNOLOGÍA

2.1 Una tecnología biométrica, dos funciones distintas

6. El reconocimiento facial es una tecnología probabilística que puede reconocer automáticamente a las personas por su rostro para autenticarlas o identificarlas.

7. La TRF se inserta en la categoría más amplia de la tecnología biométrica. La biometría incluye todos los procesos automatizados dirigidos a reconocer a un individuo mediante la cuantificación de características físicas, fisiológicas o de comportamiento (huellas dactilares, estructura del iris, voz, forma de andar, patrones de vasos sanguíneos, etc.). Estas características se definen como «datos biométricos», ya que proporcionan o confirman la identificación unívoca de dicha persona.

8. Es el caso de los rostros de las personas o, más concretamente, de su tratamiento técnico con dispositivos de reconocimiento facial: al tomar la imagen de una cara (una fotografía o un vídeo),

[1] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

llamada «muestra biométrica», es posible extraer una representación digital de características distintas de esta cara (lo que se denomina «plantilla»).

9. 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[2]. Se supone que esta plantilla es única y específica para cada persona y, en principio, es permanente a lo largo del tiempo[3]. En la fase de reconocimiento, el dispositivo compara esta plantilla con otras plantillas previamente producidas o calculadas directamente a partir de muestras biométricas, como los rostros encontrados en una imagen, foto o vídeo. El «reconocimiento facial» es, por tanto, un proceso de dos pasos: primero, la recogida de la imagen facial y su transformación en una plantilla; después, el reconocimiento de esta cara mediante la comparación de la plantilla correspondiente con una o más plantillas.

10. Como cualquier proceso biométrico, el reconocimiento facial puede cumplir dos funciones distintas:

- La **autenticación** de una persona con el fin de verificar que dicha persona es quien afirma ser. En este caso, el sistema compara una plantilla o muestra biométrica pregrabada (por ejemplo, almacenada en una tarjeta inteligente o un pasaporte biométrico) con un único rostro, como el de una persona que se presenta en un puesto de control, para verificar si se trata de la misma persona. Por lo tanto, esta función se basa en la comparación de dos plantillas. Se denomina también **verificación** de 1 a 1.

- La **identificación** de una persona con el fin de localizarla entre un grupo de individuos, dentro de un área específica, en una imagen o en una base de datos. En este caso, el sistema debe procesar cada rostro capturado para generar una plantilla biométrica y luego comprobar si coincide con una persona conocida por el sistema. Así pues, esta función se basa en la comparación de una plantilla con una base de datos de plantillas o muestras (base de referencia). Se denomina también identificación de «uno entre muchos». Por ejemplo, puede relacionar un registro de nombres personales (apellidos, nombre) con un rostro, si la comparación se hace con una base de datos de fotografías asociadas a apellidos y nombres. También puede implicar el seguimiento de una persona a través de una multitud, sin establecer necesariamente un vínculo con la identidad civil de la persona.

11. En ambos casos, 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 quien 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.

12. Aunque las dos funciones (autenticación e identificación) son distintas, ambas se refieren al tratamiento de datos biométricos relacionados con una persona física identificada o identificable y, por lo tanto, constituyen un tratamiento de datos personales y, más concretamente, un tratamiento de categorías especiales de datos personales.

13. El reconocimiento facial forma parte de un espectro más amplio de técnicas de procesamiento de imágenes de vídeo. Algunas cámaras de vídeo pueden filmar a personas dentro de un área definida,

[2] *Guidelines on facial recognition* (directrices sobre el reconocimiento facial) Comité Consultivo del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), Consejo de Europa, junio de 2021.

[3] Esto puede depender del tipo de biometría y de la edad del interesado.

en particular sus rostros, pero por sí mismas no sirven para reconocer automáticamente a los individuos. Lo mismo ocurre con la simple fotografía: una cámara no es un sistema de reconocimiento facial, ya que las fotografías de personas deben tratarse de una manera específica para poder extraer datos biométricos.

14. La mera detección de rostros por parte de las llamadas cámaras «inteligentes» tampoco constituye necesariamente un sistema de reconocimiento facial. Aunque también plantean cuestiones importantes desde el punto de vista de la ética y la eficacia, las técnicas digitales para detectar comportamientos anómalos o acontecimientos violentos, o para reconocer emociones faciales o incluso siluetas, pueden no considerarse sistemas biométricos que traten categorías especiales de datos personales, siempre que no tengan por objeto identificar de manera unívoca a una persona y que el tratamiento de datos personales en cuestión no incluya otras categorías especiales de datos personales. Estos ejemplos no están totalmente relacionados con el reconocimiento facial y permanecen sujetos a las normas de protección de datos personales.[4] Además, este tipo de sistema de detección puede utilizarse en conjunción con otros sistemas destinados a identificar a una persona y, por lo tanto, ser considerado una tecnología de reconocimiento facial.

15. A diferencia de los sistemas de captura y tratamiento de vídeo, por ejemplo, que requieren la instalación de dispositivos físicos, el reconocimiento facial es una función de software que puede implantarse en los sistemas existentes (cámaras, bases de datos de imágenes, etc.). Por lo tanto, esta función puede conectarse o interrelacionarse con una multitud de sistemas y combinarse con otras funciones. Esta integración en una infraestructura ya existente merece especial atención, pues entraña riesgos inherentes debido a la posibilidad de ocultar fácilmente la tecnología de reconocimiento facial[5].

2.2 Amplia variedad de fines y aplicaciones

16. Más allá del ámbito de aplicación de las presentes directrices y de la DAP, el reconocimiento facial puede utilizarse para múltiples objetivos, tanto de carácter comercial como en el ámbito de la seguridad pública o de la actuación policial. Puede aplicarse en muchos contextos diferentes: en la relación personal entre un usuario y un servicio (acceso a una aplicación), para acceder a un lugar específico (filtrado físico) o sin ninguna limitación particular en el espacio público (reconocimiento facial en directo). Puede aplicarse a cualquier tipo de interesado: un cliente de un servicio, un empleado, un simple espectador, una persona buscada o implicada en un procedimiento judicial o administrativo, etc. Algunos usos ya son habituales y están muy extendidos; otros se encuentran actualmente en la fase experimental o especulativa. Si bien las presentes directrices no abordan todos estos usos y aplicaciones, el CEPD recuerda que estos solo pueden llevarse a cabo si son conformes con la legislación aplicable y, en particular, el RGPD y las leyes nacionales pertinentes.[6] Incluso en el contexto de la DAP, además de las funciones de autenticación o identificación, los datos procesados con el uso de la tecnología de reconocimiento facial también pueden tratarse posteriormente para otros fines, como la clasificación.

17. Más concretamente, podría considerarse una escala de usos potenciales en función del grado de control que las personas tienen sobre sus datos personales, los medios efectivos de que disponen para ejercer dicho control y su derecho de iniciativa para activar y utilizar esta tecnología, las consecuencias

[4] Sin embargo, el artículo 10 de la DAP (o el artículo 9 del RGPD) es aplicable a los sistemas que se utilizan para clasificar a las personas en grupos, en función de sus datos biométricos, por su origen étnico, su orientación política o sexual u otras categorías especiales de datos personales.
[5] Por ejemplo, en las cada vez más utilizadas cámaras corporales.
[6] Para más orientación, véanse también las Directrices 3/2019 del CEPD sobre el tratamiento de datos personales mediante dispositivos de vídeo, adoptadas el 29 de enero de 2020.

para ellas (en caso de reconocimiento o no reconocimiento) y el alcance del tratamiento realizado. El reconocimiento facial basado en una plantilla almacenada en un dispositivo personal (tarjeta inteligente, teléfono inteligente, etc.) perteneciente a dicha persona, utilizada para la autenticación y el uso estrictamente personal a través de una interfaz específica, no plantea los mismos riesgos que, por ejemplo, el uso con fines de identificación, en un entorno no controlado, 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. Entre estos dos extremos existe un espectro muy variado de usos y cuestiones conexas relacionadas con la protección de los datos personales.

18. Para ilustrar mejor el contexto en el que se debaten o aplican actualmente las tecnologías de reconocimiento facial, ya sea para la autenticación o para la identificación, el CEPD estima pertinente mencionar una serie de ejemplos. Los ejemplos siguientes son meramente descriptivos y no deben considerarse como ningún tipo de evaluación preliminar de su conformidad con el acervo de la UE en el ámbito de la protección de datos.

Ejemplos de autenticación por reconocimiento facial

19. La autenticación puede diseñarse para que los usuarios tengan pleno control sobre ella, por ejemplo, para permitir el acceso a servicios o aplicaciones exclusivamente dentro de un entorno doméstico. Como tal, es frecuente que los propietarios de teléfonos inteligentes la utilicen para desbloquear su dispositivo, en lugar de la autenticación por contraseña.

20. La autenticación por reconocimiento facial también puede servir para comprobar la identidad de una persona que pretende recurrir a servicios de terceros públicos o privados. Así pues, estos procesos ofrecen una forma de crear una identidad digital a través de una aplicación móvil (teléfono inteligente, tableta, etc.) que puede utilizarse para acceder a servicios administrativos en línea.

21. Además, la autenticación del reconocimiento facial puede tener por objeto controlar el acceso físico a una o más ubicaciones predeterminadas, como entradas a edificios o pasos fronterizos específicos. Esta función se aplica, por ejemplo, en determinados tratamientos con fines de cruce de fronteras, en los que la cara de la persona en el dispositivo del puesto de control se compara con la almacenada en su documento de identidad (pasaporte o permiso de residencia seguro).

Ejemplos de identificación por reconocimiento facial

22. La identificación puede aplicarse de muchas maneras, incluso más diversas. En particular, se trata de los usos que se enumeran a continuación, que actualmente son objeto de observación, ensayo o planificación en la UE.

- búsqueda, en una base de datos de fotografías, de la identidad de una persona no identificada (víctima, sospechoso, etc.);
- seguimiento de los movimientos de una persona en el espacio público, para lo cual se compara su rostro con las plantillas biométricas de las personas que viajan o han viajado en la zona objeto de seguimiento, por ejemplo cuando se ha extraviado un equipaje o se ha cometido un delito;
- reconstruir el viaje de una persona y sus posteriores interacciones con otras personas, mediante una comparación retardada de los mismos elementos en un intento por identificar sus contactos, por ejemplo;

- identificación biométrica remota de las personas buscadas en espacios públicos, para lo cual todos los rostros captados en directo por las cámaras de videovigilancia se cotejan, en tiempo real, con una base de datos de las fuerzas de seguridad;

- reconocimiento automático de las personas en una imagen con el fin de identificar, por ejemplo, sus relaciones en una red social, que utiliza dicha imagen, para lo cual esta se compara con las plantillas de todos los miembros de la red que han dado su consentimiento a esta función para sugerir la identificación nominativa de estas relaciones;

- acceso a los servicios, con algunos cajeros automáticos que reconocen a sus clientes comparando un rostro captado por una cámara con la base de datos de imágenes faciales que posee el banco;

- seguimiento del viaje de un pasajero en una determinada fase del viaje, para lo cual la plantilla, calculada en tiempo real, de cualquier persona que facture en puertas situadas en determinadas etapas del viaje (puntos de entrega de equipajes, puertas de embarque, etc.) se compara con las plantillas de personas registradas previamente en el sistema.

23. Además del uso de la TRF en el ámbito de la aplicación de la ley, la amplia gama de aplicaciones observadas requiere sin duda un debate exhaustivo y un enfoque político para garantizar la coherencia y el cumplimiento del acervo de la UE en el ámbito de la protección de datos.

2.3 Fiabilidad, precisión y riesgos para los interesados

24. Como todas las tecnologías, la del reconocimiento facial también puede estar sujeta a dificultades en lo que respecta a su aplicación, en particular en lo que se refiere a su fiabilidad y eficiencia en términos de autenticación o identificación, así como a la cuestión general de la calidad y la exactitud de los datos «fuente» y el resultado del tratamiento tecnológico de reconocimiento facial.

25. Estos retos tecnológicos entrañan riesgos particulares para los interesados, riesgos que son tanto más significativos o graves en el ámbito de la aplicación de la ley, habida cuenta de los posibles efectos para los interesados, ya sean jurídicos o de otro tipo que también les afecten de manera significativa. En este contexto, parece útil subrayar asimismo que el uso *ex post* de la TRF no es de por sí más seguro, ya que las personas pueden ser objeto de seguimiento a lo largo del tiempo y en múltiples lugares. Así pues, el uso *ex post* también entraña riesgos específicos que deben valorarse caso por caso.[7]

26. Como señala la Agencia de los Derechos Fundamentales de la Unión Europea en su informe de 2019, es difícil determinar el nivel necesario de precisión del software de reconocimiento facial: existen muchas formas diferentes de evaluar y valorar la exactitud, en función de la tarea, la finalidad y el contexto de su uso, entre otros factores. Al aplicar la tecnología en lugares visitados por millones de personas, como estaciones de tren o aeropuertos, una proporción relativamente pequeña de errores (por ejemplo, el 0,01 %)[8] sigue significando que se señale erróneamente a cientos de personas. Además, determinadas categorías de personas pueden tener más probabilidades de ser emparejadas erróneamente que otras, como se describe en la sección 3. Existen diferentes maneras de calcular e interpretar las tasas de error, por lo que se requiere cautela. Además, en lo que respecta a la precisión y los errores, las cuestiones relacionadas con la facilidad con la que se puede engañar a un sistema

[7] Véanse los ejemplos expuestos en el anexo III.

[8] Esta tasa de precisión se deriva del informe citado y refleja una tasa mucho mejor que el rendimiento actual de los algoritmos en las aplicaciones de la TRF.

mediante, por ejemplo, imágenes de caras falsas (lo que se denomina *spoofing)* adquieren gran importancia, sobre todo para fines policiales.[9]

27. En este contexto, el CEPD considera importante recordar que la TRF, tanto si se utiliza con fines de autenticación como de identificación, no proporciona un resultado definitivo, sino que se basa en probabilidades de que dos rostros, o imágenes de rostros, correspondan a la misma persona.[10] Este resultado se devalúa aún más cuando la calidad de la muestra biométrica utilizada en el reconocimiento facial es baja. La borrosidad de las imágenes, la baja resolución de la cámara, el movimiento y la poca luz pueden ser factores de baja calidad. Otros aspectos con un impacto significativo en los resultados son la prevalencia y la suplantación de identidad, por ejemplo, cuando los delincuentes intentan evitar pasar por delante de las cámaras o engañar a la TRF. Numerosos estudios también han puesto de relieve que estos resultados estadísticos del tratamiento algorítmico también pueden estar sujetos a sesgos, en particular derivados de la calidad de los datos de origen, así como de las bases de datos de entrenamiento, o de otros factores, como la elección de la ubicación. Además, también hay que destacar el impacto de la tecnología de reconocimiento facial en otros derechos fundamentales, como el respeto a la vida privada y familiar, la libertad de expresión e información, la libertad de reunión y asociación, etc.

28. Por lo tanto, es esencial que la fiabilidad y la exactitud de la tecnología de reconocimiento facial se tengan en cuenta como criterios para evaluar el cumplimiento de los principios clave de protección de datos, de conformidad con el artículo 4 de la DAP, y en particular en lo que se refiere a la equidad y la exactitud.

29. Al tiempo que destaca que unos datos de alta calidad son esenciales para unos algoritmos de alta calidad, el CEPD también subraya la necesidad de que los responsables del tratamiento de datos, como parte de su obligación de rendición de cuentas, lleven a cabo una evaluación periódica y sistemática del tratamiento algorítmico con el fin de garantizar, en particular, la exactitud, la imparcialidad y la fiabilidad del resultado de dicho tratamiento. Los datos personales utilizados con fines de evaluación, entrenamiento y perfeccionamiento de los sistemas de TRF solo deben tratarse sobre la base de un fundamento jurídico suficiente y de conformidad con los principios comunes de protección de datos.

3 MARCO JURÍDICO APLICABLE

30. El uso de tecnologías de reconocimiento facial está intrínsecamente vinculado al tratamiento de datos personales, incluidas las categorías especiales de datos. Además, tiene un impacto directo o indirecto en una serie de derechos fundamentales, consagrados en la Carta de los Derechos Fundamentales de la UE. Esto es especialmente relevante en el ámbito de la aplicación de la ley y la justicia penal. Por lo tanto, cualquier uso de tecnologías de reconocimiento facial debe llevarse a cabo en estricto cumplimiento de la legislación aplicable.

31. La siguiente información está destinada a ser tenida en cuenta a la hora de estudiar futuras medidas legislativas y administrativas y en toda aplicación concreta de la legislación vigente relacionada con la TRF. La pertinencia de los distintos requisitos varía en función de las circunstancias particulares. Dado

[9] *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (Tecnología de reconocimiento facial: consideraciones de los derechos fundamentales en el contexto de la aplicación de la ley), Agencia de los Derechos Fundamentales de la UE, 21 de noviembre de 2019.
[10] Esta probabilidad se denomina «grado de certeza».

que no se pueden prever todas las circunstancias futuras, la siguiente información es meramente ilustrativa y no debe interpretarse como una enumeración exhaustiva.

3.1 Marco jurídico general – La Carta de los Derechos Fundamentales de la UE y el Convenio Europeo de Derechos Humanos (CEDH)

3.1.1 Aplicabilidad de la Carta

32. La Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «la Carta») se dirige a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros cuando aplican el Derecho de la Unión.

33. La regulación del tratamiento de datos biométricos con fines policiales con arreglo al artículo 1, apartado 1, de la DAP plantea inevitablemente la cuestión del respeto de los derechos fundamentales, en particular el respeto de la vida privada y las comunicaciones, consagrado en el artículo 7 de la Carta, y el derecho a la protección de los datos de carácter personal, reconocido por el artículo 8 de la Carta.

34. La recogida y el análisis de imágenes de vídeo de las personas físicas, incluidas sus caras, implica el tratamiento de datos personales. Al procesar técnicamente la imagen, el tratamiento abarca también los datos biométricos. El tratamiento técnico de los datos relativos a la cara de una persona física en relación con el tiempo y el lugar permite extraer conclusiones sobre la vida privada de las personas afectadas. Estas conclusiones pueden referirse a los orígenes raciales o étnicos, la salud, la religión, los hábitos de la vida cotidiana, el lugar de residencia habitual o temporal, los desplazamientos diarios o de otro tipo, las actividades realizadas, las relaciones sociales y los entornos sociales frecuentados. La gran variedad de información que puede revelar la aplicación de la TRF muestra claramente el posible impacto en el derecho a la protección de los datos personales consagrado en el artículo 8 de la Carta, pero también en el derecho a la intimidad protegido por el artículo 7 de la Carta.

35. En tales circunstancias, tampoco es inconcebible que la recogida, el análisis y el posterior tratamiento de los datos biométricos (faciales) en cuestión puedan tener un efecto sobre la sensación de libertad de las personas para actuar, incluso cuando su conducta sea plenamente lícita en una sociedad libre y abierta. También puede tener graves repercusiones en el ejercicio de los derechos fundamentales, como el derecho a la libertad de pensamiento, de conciencia y de religión, a la libertad de expresión y a la libertad de reunión pacífica y de asociación en virtud de los artículos 1, 10, 11 y 12 de la Carta. Dicho tratamiento también implica otros riesgos, como el riesgo de uso indebido de la información personal recogida por las autoridades pertinentes como resultado del acceso y uso ilícitos de los datos personales, la violación de la seguridad, etc. Con frecuencia, los riesgos dependen del tratamiento y de sus circunstancias, como el riesgo de acceso y uso ilícitos por parte de los agentes de policía u otras personas no autorizadas. Sin embargo, algunos riesgos simplemente son inherentes a la naturaleza única de los datos biométricos. A diferencia de la dirección o el número de teléfono, es imposible que un interesado cambie sus rasgos personales, como el rostro o el iris. En caso de acceso no autorizado o publicación accidental de datos biométricos, esto supondría que los datos se verían comprometidos en su uso como contraseñas o claves criptográficas, o podrían utilizarse para otras actividades de vigilancia no autorizadas en detrimento del interesado.

3.1.2 Interferencia con los derechos establecidos en la Carta

36. El tratamiento de datos biométricos constituye en sí mismo una grave injerencia en cualquier circunstancia y con independencia del resultado (por ejemplo, de una coincidencia encontrada). El

tratamiento constituye una interferencia incluso si la plantilla biométrica se suprime inmediatamente después de que la comparación con una base de datos policial dé lugar a una respuesta negativa.

37. La injerencia en los derechos fundamentales de los interesados puede derivarse de un acto jurídico que tenga por objeto o por efecto restringir el derecho fundamental de que se trate[11]. También puede ser el resultado de un acto de una autoridad pública con el mismo objeto o efecto, o incluso de una entidad privada a la que la ley haya encomendado el ejercicio de la autoridad pública y los poderes públicos.

38. Una medida legislativa que sirve de base jurídica para el tratamiento de datos personales interfiere directamente con los derechos garantizados por los artículos 7 y 8 de la Carta[12].

39. El uso de datos biométricos, y de la TRF en particular, en muchos casos también afecta al derecho a la dignidad humana, garantizado por el artículo 1 de la Carta. La dignidad humana exige que las personas no sean tratadas como meros objetos. La TRF calcula características existenciales y muy personales, los rasgos faciales, en un formato legible por máquina con el fin de utilizarlo como matrícula o carné de identidad humano, cosificando así el rostro.

40. Dicho tratamiento también puede interferir con otros derechos fundamentales, como los derechos contemplados en los artículos 10, 11 y 12 de la Carta, en la medida en que los efectos intimidatorios estén previstos o se deriven de la videovigilancia pertinente de las fuerzas y cuerpos de seguridad.

41. Además, también deben estudiarse detenidamente los riesgos potenciales que genera el uso de tecnologías de reconocimiento facial por parte de las fuerzas del orden en relación con el derecho a un juicio justo y la presunción de inocencia en virtud de los artículos 47 y 48 de la Carta. El resultado de la aplicación de la TRF, por ejemplo, una coincidencia, puede no solo llevar a que una persona sea objeto de actuaciones policiales, sino que también puede servir de prueba decisiva en un procedimiento judicial. Por lo tanto, las deficiencias de la TRF, como el posible sesgo, la discriminación o la identificación incorrecta («falso positivo»), pueden tener graves consecuencias también en los procedimientos penales. Además, en la evaluación de las pruebas puede favorecerse el resultado de la aplicación de la TRF, aun existiendo pruebas contradictorias («sesgo de automatización»).

3.1.3 Justificación de la injerencia

42. A tenor del artículo 52, apartado 1, de la Carta, toda limitación al ejercicio de los derechos y libertades fundamentales debe estar prevista por la ley y respetar la esencia de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, solo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión Europea o a la necesidad de protección de los derechos y libertades de los demás.

3.1.3.1 Prevista por la ley

43. El artículo 52, apartado 1, de la Carta establece el requisito de una base legal específica. Esta base legal debe ser suficientemente clara en sus términos para proporcionar a los ciudadanos una indicación adecuada de las condiciones y circunstancias en las que las autoridades están facultadas para recurrir a una medida de recogida de datos y vigilancia secreta[13]. Debe indicar con una claridad razonable el alcance y las modalidades de ejercicio de la correspondiente facultad discrecional conferida a las autoridades públicas, a fin de garantizar a los particulares el mínimo grado de protección que le

[11] TJUE, C-219/91 – Ter Voort, RoC 1992 I-05485, apartados 36 y 37; TJUE, C-200/96 – Metronome, RoC 1998 I-1953, apartado 28.
[12] TJUE, C-594/12, apartado 36; TJUE, C-291/12, apartados 23 y siguientes.
[13] TEDH, Shimovolos c. Rusia, § 68; Vukota-Bojić c. Suiza.

confiere el Estado de Derecho en una sociedad democrática[14]. Además, la legalidad requiere salvaguardias adecuadas para garantizar que se respete, en particular, el derecho individual reconocido en el artículo 8 de la Carta. Estos principios también se aplican al tratamiento de datos personales con fines de evaluación, entrenamiento y ulterior desarrollo de los sistemas de TRF.

44. Dado que los datos biométricos tratados con el fin de identificar de manera unívoca a una persona física constituyen categorías especiales de datos enumeradas en el artículo 10 de la DAP, en la mayoría de los casos las diferentes aplicaciones de la TRF requerirían una ley específica que describa con precisión la solicitud y las condiciones para su uso. Esto incluye, en particular, los tipos de delitos y, en su caso, el umbral adecuado de gravedad de estos delitos, en particular con el fin de excluir de manera efectiva los delitos menores.[15]

3.1.3.2 La esencia del derecho fundamental a la intimidad y a la protección de los datos personales, consagrado en los artículos 7 y 8 de la Carta

45. Las limitaciones de los derechos fundamentales inherentes a cada situación aún deben respetar el contenido esencial del derecho concreto. Este contenido esencial se refiere al núcleo mismo del derecho fundamental[16]. Asimismo, se ha de respetar la dignidad humana, incluso en el caso de limitación de un derecho[17].

46. Los indicios de una posible infracción del núcleo inviolable son los siguientes:

- Una disposición que impone limitaciones independientemente de la conducta individual de una persona o de circunstancias excepcionales[18].
- No se permite o se dificulta el acceso a los tribunales[19].
- Antes de imponer una limitación grave, no se tienen en cuenta las circunstancias de la persona afectada[20].
- En relación con los derechos consagrados en los artículos 7 y 8 de la Carta: además de una amplia recopilación de metadatos de comunicación, la adquisición del conocimiento del contenido de la comunicación electrónica podría vulnerar la esencia de dichos derechos[21].
- En relación con los derechos consagrados en los artículos 7, 8 y 11 de la Carta: una legislación que exige que los proveedores de acceso a los servicios públicos de comunicaciones en línea y los proveedores de servicios de alojamiento de datos conserven, de manera general e indiscriminada, entre otras cosas, los datos personales relativos a dichos servicios[22].
- En relación con los derechos consagrados en el artículo 8 de la Carta: la ausencia de principios básicos de protección de datos y seguridad de los datos también podría vulnerar el núcleo del derecho[23].

[14] TEDH, Piechowicz c. Polonia, § 212.
[15] Véanse, por ejemplo, las sentencias del TJUE en los asuntos C-817/19, Ligue des droits humains, apartados 151 y 152, y C-207/16, Ministerio Fiscal, apartado 56.
[16] TJUE C-279/09, RoC 2010 I-13849, apartado 60.
[17] Explicaciones sobre la Carta de los Derechos Fundamentales, título I, Explicación relativa al artículo 1, DO C 303 de 14.12.2007, pp. 17-35.
[18] TJUE C-601/15, apartado 52.
[19] TJUE C-400/10, RoC 2010 I-08965, apartado 55.
[20] TJUE C-408/03, RoC 2006 I-02647, apartado 68.
[21] TJUE: 203/15 - Tele2 Sverige, apartado 101, con remisión a TJUE: C-293/12 y C-594/12, apartado 39.
[22] TJUE C-512/18, La Quadrature du Net, apartados 209 y apartados.
[23] TJUE: C-594/12, apartado 40.

3.1.3.3 Objetivo legítimo

47. Como ya se ha explicado en el punto 3.1.3., las limitaciones a los derechos fundamentales deben responder efectivamente a objetivos de interés general reconocidos por la Unión Europea o a la necesidad de proteger los derechos y libertades de los demás.

48. La Unión reconoce tanto los objetivos mencionados en el artículo 3 del Tratado de la Unión Europea como otros intereses protegidos por disposiciones específicas de los Tratados[24], en particular, un espacio de libertad, seguridad y justicia y la prevención y lucha contra la delincuencia. En sus relaciones con el resto del mundo, la Unión debe contribuir a la paz y la seguridad y a la protección de los derechos humanos.

49. La necesidad de proteger los derechos y libertades de los demás se refiere a los derechos de las personas que están protegidos por la legislación de la Unión Europea o de sus Estados miembros. La evaluación debe llevarse a cabo con el fin de conciliar las exigencias de la protección de los derechos respectivos y lograr un justo equilibrio entre ellos[25].

3.1.3.4 Prueba de necesidad y proporcionalidad

50. Cuando estén en juego injerencias en los derechos fundamentales, el alcance de la discrecionalidad del legislador nacional y de la Unión puede resultar limitado. Esto depende de una serie de factores, entre ellos el ámbito de que se trate, la naturaleza del derecho en cuestión garantizado por la Carta, la naturaleza y la gravedad de la injerencia y el objetivo perseguido por esta[26]. Las medidas legislativas deben ser adecuadas para alcanzar los objetivos legítimos perseguidos por la legislación en cuestión. Además, la medida no debe exceder los límites de lo adecuado y necesario para alcanzar dichos objetivos[27]. Un objetivo de interés general, por esencial que sea, no justifica, por sí solo, la limitación de un derecho fundamental[28].

51. Según reiterada jurisprudencia del TJUE, las excepciones y limitaciones en relación con la protección de los datos personales solo deben aplicarse en la medida estrictamente necesaria[29]. Esto implica también que no existan otros medios menos gravosos para alcanzar el fin propuesto. Se han de estudiar y evaluar cuidadosamente posibles alternativas, como (en función del objetivo de que se trate) el refuerzo del personal o de la vigilancia policial o un mayor alumbrado público. Las medidas legislativas deben diferenciar y dirigirse a las personas afectadas teniendo en cuenta el objetivo; por ejemplo, la lucha contra la delincuencia grave. Si se dirigen a todas las personas con carácter general, sin tal diferenciación, limitación o excepción, la injerencia se ve agravada[30]. Lo mismo sucede si el tratamiento de datos afecta a una parte significativa de la población[31].

---

[24] Explicaciones sobre la Carta de los Derechos Fundamentales, título I, Explicación relativa al artículo 52, DO C 303 de 14.12.2007, pp. 17-35.
[25] Jarass GrCh, 3ª ed. 2016, EU-Grundrechte-Charta, artículo 52, apartados 31-32.
[26] TJUE: C-594/12, apartado 47 con las siguientes fuentes: véanse, por analogía, en lo que respecta al artículo 8 del CEDH, TEDH, S. y Marper c. Reino Unido [GS], n.º 30562/04 y n.º 30566/04, § 102, ECHR 2008-V.
[27] TJUE: C-594/12, apartado 46 con las siguientes fuentes: asunto C-343/09, Afton Chemical EU:C:2010:419, apartado 45; Volker und Markus Schecke y Eifert EU:C:2010:662, apartado 74; asuntos C-581/10 y C-629/10 Nelson y otros, EU:C:2012:657, apartado 71; asunto C-283/11, Sky Österreich EU:C:2013:28, apartado 50, y asunto C-101/12, Schaible EU:C:2013:661, apartado 29.
[28] TJUE: C-594/12, apartado 51.
[29] TJUE: C-594/12, apartado 52, con las siguientes fuentes: asunto C-473/12 IPI, EU:C:2013:715, apartado 39 y la jurisprudencia citada.
[30] TJUE: C-594/12, apartado 57.
[31] TJUE: C-594/12, apartado 56.

52. La protección de los datos personales derivada de la obligación explícita establecida en el artículo 8, apartado 1, de la Carta es especialmente importante para el derecho de respeto de la vida privada consagrado en el artículo 7 de la Carta[32]. La legislación debe establecer normas claras y precisas que regulen el alcance y la aplicación de la medida de que se trate y debe imponer garantías para que las personas cuyos datos hayan sido tratados cuenten con medios suficientes para proteger eficazmente sus datos personales contra el riesgo de abuso y contra cualquier acceso o utilización ilícitos de dichos datos[33]. La necesidad de tales garantías es aún mayor cuando los datos personales son objeto de tratamiento automatizado y cuando existe un riesgo significativo de acceso ilícito a los datos[34]. Además, la autorización interna o externa, por ejemplo judicial, del despliegue de la TRF también puede contribuir como garantía y puede resultar necesaria en determinados casos de interferencias graves.[35]

53. Las normas establecidas deben adaptarse a la situación específica, por ejemplo, la cantidad de datos tratados, la naturaleza de los datos[36] y el riesgo de acceso ilícito a los datos. Esto requiere normas que sirvan, en particular, para regular la protección y la seguridad de los datos en cuestión de manera clara y estricta, a fin de garantizar su plena integridad y confidencialidad[37].

54. Por lo que respecta a la relación entre el responsable y el encargado del tratamiento, no debe permitirse que los encargados del tratamiento tengan en cuenta únicamente consideraciones económicas a la hora de determinar el nivel de seguridad que aplican a los datos personales; esto podría poner en peligro un nivel de protección suficientemente elevado[38].

55. Mediante ley se deben establecer las condiciones sustantivas y procesales y los criterios objetivos para determinar los límites del acceso de las autoridades competentes a los datos y su ulterior uso. A efectos de prevención, detección o enjuiciamiento penal, los delitos habrían de considerarse suficientemente graves para justificar el alcance y la gravedad de estas injerencias en los derechos fundamentales consagrados; por ejemplo, en los artículos 7 y 8 de la Carta[39].

56. Los datos deben tratarse de manera que se garantice la aplicabilidad y el efecto de las normas de protección de datos de la UE; en particular, las previstas en el artículo 8 de la Carta, que establece que el cumplimiento de los requisitos de protección y seguridad estará sujeto al control de una autoridad independiente. En tal situación puede ser relevante el lugar geográfico donde tenga lugar el tratamiento[40].

57. Por lo que respecta a las diferentes fases del tratamiento de datos personales, debe diferenciarse entre las categorías de datos en función de su posible utilidad para los fines del objetivo perseguido o según las personas afectadas[41]. La determinación de las condiciones del tratamiento (por ejemplo, el período

[32] TJUE: C-594/12, apartado 53.
[33] TJUE: C-594/12, apartado 54, con las siguientes fuentes: véase, por analogía, respecto al artículo 8 del CEDH, TEDH: Liberty y otros c. Reino Unido, 1 de julio de 2008, n.º 58243/00, §§ 62 y 63; Rotaru c. Rumanía, §§ 57 a 59, y S. y Marper c. Reino Unido, § 99.
[34] TJUE: C-594/12, apartado 55, con las siguientes fuentes: véanse, por analogía, en lo que respecta al artículo 8 del CEDH, S. y Marper c. Reino Unido, § 103, y M. K. c. Francia, 18 de abril de 2013, n.º 19522/09, § 35.
[35] TEDH, Szabó y Vissy c. Hungría, §§ 73-77.
[36] Véanse también los requisitos más estrictos para las medidas técnicas y organizativas en el tratamiento de categorías especiales de datos (artículo 29, apartado 1, de la DAP).
[37] TJUE: C-594/12, apartado 66.
[38] TJUE: C-594/12, apartado 67.
[39] TJUE: C-594/12, apartados 60 y 61.
[40] TJUE: C-594/12, apartado 68.
[41] TJUE: C-594/12, apartado 63.

de conservación) debe basarse en criterios objetivos, para garantizar que la injerencia se limite a lo estrictamente necesario[42].

58. Atendiendo a cada situación concreta, la evaluación de la necesidad y la proporcionalidad debe identificar y considerar todas las posibles repercusiones en el ámbito de otros derechos fundamentales, como la dignidad humana en virtud del artículo 1 de la Carta, la libertad de pensamiento, de conciencia y de religión en virtud del artículo 10 de la Carta, la libertad de expresión en virtud del artículo 11 de la Carta y la libertad de reunión y de asociación en virtud del artículo 12 de la Carta.

59. Además, debe considerarse como un factor de gravedad que, si el tratamiento de los datos se produce sistemáticamente sin el conocimiento de los interesados, es probable que genere una sensación general de vigilancia constante[43]. Esto puede provocar un efecto intimidatorio en relación con los derechos fundamentales afectados.

60. Con el fin de facilitar y poner en práctica la evaluación de la necesidad y proporcionalidad de las medidas legislativas relacionadas con el reconocimiento facial en el ámbito policial, los legisladores nacionales y de la Unión pueden aprovechar las herramientas prácticas disponibles especialmente diseñadas para esta tarea. En particular, podría utilizarse el conjunto de herramientas de necesidad y proporcionalidad[44] proporcionado por el Supervisor Europeo de Protección de Datos.

3.1.3.5 Artículos 52, apartado 3, y 53 de la Carta (nivel de protección, también en relación con el del CEDH)

61. Con arreglo a los artículos 52, apartado 3, y 53 de la Carta, el significado y el alcance de los derechos de la Carta que corresponden a los derechos garantizados en el CEDH deben ser los mismos que los establecidos por el CEDH. Si bien, en particular, en el caso del artículo 7 de la Carta puede encontrarse un equivalente en el CEDH, este no es el caso del artículo 8 de la Carta[45]. El artículo 52, apartado 3, de la Carta no se opone a que el Derecho de la Unión confiera una protección más amplia. Dado que el CEDH no constituye un instrumento jurídico que se haya incorporado formalmente al Derecho de la UE, la legislación de la UE debe adoptarse a la luz de los derechos fundamentales de la Carta[46].

62. De conformidad con el artículo 8 del CEDH, no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho excepto en la medida en que esta injerencia esté prevista por la ley y sea necesaria en una sociedad democrática para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

63. El CEDH también establece normas relativas a la forma en que pueden imponerse las limitaciones. Un requisito básico, además del principio de legalidad, es la previsibilidad. Para cumplir la exigencia de previsibilidad, la legislación nacional debe ser suficientemente clara para ofrecer a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades públicas están

[42] TJUE: C-594/12, apartado 64.
[43] TJUE: C-594/12, apartado 37.
[44] Supervisor Europeo de Protección de Datos: *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit* (Conjunto de herramientas para evaluar la necesidad de medidas que limiten el derecho fundamental a la protección de los datos personales) (11.4.2017); Supervisor Europeo de Protección de Datos: Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales (19.12.2019).
[45] TJUE: C-203/15 - Tele2 Sverige, apartado 129.
[46] TJUE: C-311/18, apartado 99.

facultadas para recurrir a tales medidas.[47] Este requisito está reconocido por el TJUE y por la legislación de protección de datos de la UE (véase la sección 3.2.1.1).

64. Además de especificar los derechos del artículo 8 del CEDH, también deben respetarse plenamente las disposiciones del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[48]. No obstante, hay que tener en cuenta que estas disposiciones solo constituyen normas mínimas a efectos del Derecho de la Unión vigente.

3.2 Marco jurídico específico: la Directiva sobre protección de datos en el ámbito penal

65. En la DAP se establece un determinado régimen relativo a la utilización de la TRF. En primer lugar, el artículo 3, punto 13, de la DAP define el concepto de «datos biométricos»[49]. Para más detalles, véase el apartado 2.1. En segundo lugar, el artículo 8, apartado 2, aclara que, para que un tratamiento sea lícito, además de ser necesario para los fines indicados en el artículo 1, apartado 1, debe estar regulado en una legislación nacional que especifique, al menos, los objetivos del tratamiento, los datos personales que se van a tratar y la finalidad del tratamiento. Otras disposiciones de especial relevancia en relación con los datos biométricos son los artículos 10 y 11 de la DAP. El artículo 10 debe leerse en relación con el artículo 8 de la DAP[50]. Siempre deben respetarse los principios para el tratamiento de datos personales establecidos en el artículo 4 de la DAP, y cualquier evaluación del posible tratamiento biométrico mediante la TRF debe guiarse por ellos.

3.2.1 Tratamiento de categorías especiales de datos con fines de aplicación de la ley

66. A tenor del artículo 10 de la DAP, el tratamiento de categorías especiales de datos, como los datos biométricos, solo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado. Además, solo se permitirá cuando lo autorice el Derecho de la Unión o del Estado miembro, cuando sea necesario para proteger los intereses vitales del interesado o de otra persona física o cuando dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos. Esta cláusula general pone de relieve la sensibilidad del tratamiento de categorías especiales de datos.

3.2.1.1 Autorizado por el Derecho de la Unión o del Estado miembro

67. En cuanto al tipo de medida legislativa necesaria, el considerando 33 de la DAP afirma que «las referencias de la presente Directiva al Derecho de un Estado miembro, a una base jurídica o a una medida legislativa no requieren necesariamente la existencia de un acto legislativo adoptado por un Parlamento, sin perjuicio de los requisitos exigidos por el ordenamiento constitucional del Estado miembro de que se trate».[51]

---

[47] Tribunal Europeo de Derechos Humanos, sentencia, Copland c. Reino Unido, 3.4.2007, solicitud n.º 62617/00, apartado 46.

[48] ETS n.º 108.

[49] Artículo 3, apartado 13, de la DAP: «datos biométricos» son datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

[50] WP 258, Dictamen sobre algunas cuestiones clave de la DAP (UE 2016/680), p. 7.

[51] El tipo de medidas legislativas consideradas tiene que estar en consonancia con el Derecho de la Unión o del Estado miembro. Dependiendo del grado de interferencia de la restricción, puede ser necesaria una medida legislativa concreta a escala nacional, teniendo en cuenta el nivel de la norma.

68. De conformidad con el artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta deberá ser «establecida por la ley». Esta expresión recuerda a la utilizada en el artículo 8, apartado 2, del Convenio Europeo de Derechos Humanos: «prevista por la ley», lo que significa no solo el cumplimiento de la legislación nacional, sino también la calidad de dicha ley, que exige su compatibilidad con el principio de legalidad.

69. Por otro lado, el considerando 33 de la DAP declara que, «no obstante, dicho Derecho de un Estado miembro, base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para quienes estén sujetos a la misma, tal y como exige la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos. Cuando en el Derecho de un Estado miembro se regule el tratamiento de los datos personales dentro del ámbito de aplicación de la presente Directiva, se deben indicar al menos los objetivos del tratamiento, los datos personales que serán objeto del mismo, la finalidad del tratamiento, los procedimientos para el mantenimiento de la integridad y la confidencialidad de los datos personales y los procedimientos para su destrucción […]»

70. La legislación nacional debe ser suficientemente clara para ofrecer a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que los responsables están facultados para recurrir a tales medidas. Esto incluye posibles condiciones previas para el tratamiento, como tipos específicos de pruebas, así como la necesidad de una autorización judicial o interna. La legislación correspondiente puede ser neutra desde el punto de vista tecnológico, en la medida en que se aborden suficientemente los riesgos y características específicos del tratamiento de datos personales por parte de los sistemas de TRF. En consonancia con la DAP y la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) y del Tribunal Europeo de Derechos Humanos (TEDH), es realmente esencial que las medidas legislativas, cuyo objetivo es proporcionar una base jurídica para las medidas de reconocimiento facial, sean previsibles para los interesados.

71. Una medida legislativa no puede invocarse como ley que autorice el tratamiento de datos biométricos a través de la TRF con fines policiales si se trata de una mera transposición de la cláusula general del artículo 10 de la DAP.

72. Aparte de los datos biométricos, el artículo 10 de la DAP regula el tratamiento de otras categorías especiales de datos, como la orientación sexual, las opiniones políticas y las creencias religiosas, abarcando así una amplia gama de tratamientos. Además, tal disposición carecería de unos requisitos específicos que indicasen las circunstancias y condiciones en las que los cuerpos y fuerzas de seguridad estarían facultadas para recurrir al uso de la tecnología de reconocimiento facial. Debido a la referencia a otros tipos de datos y a la necesidad explícita de garantías especiales sin más especificaciones, una disposición nacional que transponga el artículo 10 de la DAP en el Derecho nacional (con una redacción igualmente general y abstracta) no podría invocarse como base jurídica para el tratamiento de datos biométricos que implicasen el reconocimiento facial, ya que carecería de precisión y previsibilidad. De conformidad con los artículos 28, apartado 2, o 46, apartado 1, letra c), de la DAP, antes de que el legislador establezca una nueva base jurídica para cualquier forma de tratamiento de datos biométricos mediante reconocimiento facial, debe consultarse a la autoridad nacional de control de la protección de datos.

3.2.1.2 Estrictamente necesario

73. El tratamiento solo puede considerarse «estrictamente necesario» si la injerencia en la protección de los datos personales y sus restricciones se limitan a lo que es absolutamente necesario[52]. Con la adición

[52] Jurisprudencia reiterada sobre el derecho fundamental al respeto de la vida privada, véase TJUE, asunto C-73/07, apartado 56 (Satakunnan Markkinapörssi y Satamedia); TJUE, asuntos C-92/09 y C-93/09, apartado 77

del término «estrictamente», el legislador quiso que el tratamiento de categorías especiales de datos solo tuviera lugar en condiciones aún más estrictas que las de mera necesidad (véase el punto 3.1.3.4). Este requisito debe entenderse como indispensable. Limita a un mínimo absoluto el margen de apreciación que asiste a la autoridad policial en cuanto a la necesidad. De conformidad con la jurisprudencia reiterada del TJUE, la condición de «necesidad estricta» también está estrechamente vinculada al requisito de criterios objetivos para definir las circunstancias y las condiciones en las que puede llevarse a cabo el tratamiento, excluyendo así cualquier tratamiento de carácter general o sistemático[53].

3.2.1.3 Hechos manifiestamente públicos

74. Al valorar si el tratamiento se refiere a datos hechos manifiestamente públicos por el interesado, conviene recordar que una fotografía como tal no se considera por sistema un dato biométrico[54]. Así pues, el hecho de que una fotografía haya sido manifiestamente publicada por el interesado no implica que los datos biométricos correspondientes que puedan obtenerse de ella por medios técnicos específicos se consideren manifiestamente publicados.

75. En cuanto a los datos personales en general, para que los datos biométricos se consideren manifiestamente hechos públicos por el interesado, este debe haber hecho deliberadamente que la plantilla biométrica (y no simplemente una imagen facial) sea libremente accesible y pública a través de una fuente abierta. Si un tercero divulga los datos biométricos, no puede considerarse que el interesado haya hecho manifiestamente públicos los datos.

76. Además, no basta con interpretar el comportamiento de un interesado para considerar que los datos biométricos se han hecho manifiestamente públicos. Por ejemplo, en el caso de las redes sociales o las plataformas en línea, el CEPD considera que el hecho de que el interesado no haya activado o configurado características específicas de privacidad no es suficiente para considerar que haya hecho manifiestamente públicos sus datos personales y que estos (por ejemplo, fotografías) puedan tratarse en plantillas biométricas y utilizarse con fines de identificación sin el consentimiento del interesado. En términos más generales, la configuración por defecto de un servicio (como la puesta a disposición del público de plantillas o la ausencia de elección, por ejemplo, si las plantillas se hacen públicas sin que el usuario pueda modificar esta configuración) no deben interpretarse en modo alguno como datos hechos manifiestamente públicos.

3.2.2 Toma automatizada de decisiones individuales, incluida la elaboración de perfiles

77. El artículo 11, apartado 1, de la DAP impone a los Estados miembros la obligación de prohibir con carácter general las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente. Como excepción a esta prohibición general, dicho tratamiento solo podrá ser lícito si está autorizado por el Derecho de la Unión o del Estado miembro al que esté sujeto el responsable del tratamiento y que establezca garantías adecuadas para los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento. Solo puede utilizarse de forma restrictiva, limitación que se aplica a las categorías ordinarias (es decir, no

(Schecke y Eifert); TJUE, asunto C-594/12, apartado 52 (Digital Rights); TJUE, asunto C-362/14, apartado 92 (Schrems).

[53] TJUE: asunto C-623/17, apartado 78.

[54] Véase el considerando 51 del RGPD: «El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.»

especiales) de datos personales. Se impone una limitación aún más estricta y un uso más restrictivo para la exención prevista en el artículo 11, apartado 2, de la DAP, que vuelve a insistir en que las decisiones adoptadas en virtud del apartado 1 no se basarán en categorías especiales de datos, es decir, en particular, datos biométricos, con el fin de identificar de manera unívoca a una persona física. Solo podrá preverse una excepción si se aplican medidas adecuadas para proteger los derechos y libertades del interesado y los intereses legítimos de la persona física de que se trate. Esta excepción debe entenderse con carácter adicional y a la luz de las exigencias del artículo 10 de la DAP.

78. Dependiendo del sistema de TRF, incluso la intervención humana que evalúa los resultados de la TRF puede no ofrecer por sí misma una garantía suficiente en cuanto al respeto de los derechos de las personas y, en particular, del derecho a la protección de los datos personales, teniendo en cuenta los posibles sesgos y errores que pueden derivarse del propio tratamiento. Además, la intervención humana solo puede considerarse una garantía si la persona que interviene puede cuestionar de manera crítica los resultados de la TRF durante la intervención humana. Es fundamental capacitar a dicha persona para que comprenda el sistema de TRF y sus limitaciones y para que interprete correctamente sus resultados. También es necesario establecer un puesto de trabajo y una organización que contrarresten los efectos del sesgo de la automatización y eviten fomentar la aceptación no crítica de los resultados, por ejemplo, a causa de la presión del tiempo, procedimientos gravosos, posibles efectos perjudiciales para la carrera profesional, etc.

79. Con arreglo al artículo 11, apartado 3, de la DAP, la elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales quedará prohibida, de conformidad con el Derecho de la Unión. Según el artículo 3, apartado 4, de la DAP, por «elaboración de perfiles» se entiende toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. Para considerar si se han adoptado medidas adecuadas para proteger los derechos y libertades del interesado y los intereses legítimos de la persona física de que se trate, hay que tener en cuenta que el uso de la TRF puede dar lugar a la elaboración de perfiles, dependiendo de la forma y la finalidad para las que se solicite la TRF. En cualquier caso, de conformidad con el Derecho de la Unión y el artículo 11, apartado 3, de la DAP, está prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales.

3.2.3 Categorías de los interesados

80. El artículo 6 de la DAP se refiere a la necesidad de distinguir entre las diferentes categorías de interesados. Esta distinción debe hacerse cuando sea aplicable y en la medida de lo posible. Tiene que surtir efecto en la forma en que se tratan los datos. De los ejemplos que figuran en el artículo 6 de la DAP se puede deducir que, por regla general, el tratamiento de datos personales debe cumplir los criterios de necesidad y proporcionalidad también en lo que respecta a la categoría de interesados[55]. También se deduce que, en relación con los interesados para los que no existen pruebas que puedan sugerir que su conducta podría tener una relación, incluso indirecta o remota, con el objetivo legítimo según la DAP, lo más probable es que no exista justificación alguna para una injerencia[56]. Si no es aplicable o posible ninguna distinción con arreglo al artículo 6 de la DAP, la excepción a la norma del artículo 6 de la DAP debe considerarse de forma rigurosa al valorar la necesidad y la proporcionalidad

[55] Véase también TJUE: C-594/12, apartados 56 a 59.
[56] Véase también TJUE: C-594/12, apartado 58.

de la injerencia. La distinción entre las diferentes categorías de interesados parece un requisito esencial cuando se trata del tratamiento de datos personales que implica el reconocimiento facial, teniendo en cuenta también los posibles resultados falsos positivos o falsos negativos, que pueden tener repercusiones significativas para los interesados, así como en el curso de una investigación.

81. Como ya se ha dicho, al aplicar el Derecho de la Unión deben respetarse las disposiciones de la Carta de los Derechos Fundamentales de la Unión Europea (véase el artículo 52 de la Carta). Por consiguiente, el marco y los criterios que establece la DAP deben interpretarse a la luz de la Carta. Los actos jurídicos de la UE y de sus Estados miembros no deben quedar por debajo de esta medida y deben garantizar la plena efectividad de la Carta.

3.2.4 Derechos del interesado

82. El CEPD ya ha proporcionado orientaciones sobre los derechos de los interesados en virtud del RGPD en diferentes aspectos[57]. La DAP confiere derechos similares a los interesados, y se han facilitado orientaciones generales al respecto en un dictamen del Grupo de Trabajo del artículo 29, que ha sido refrendado por el CEPD[58]. En determinadas circunstancias, la DAP permite algunas limitaciones a estos derechos. Los parámetros de dichas limitaciones se detallan en el apartado 3.2.4.6. «Limitaciones legítimas de los derechos del interesado».

83. Aunque todos los derechos de los interesados enumerados en el capítulo III de la DAP naturalmente se aplican también al tratamiento de datos personales a través de la tecnología de reconocimiento facial (TRF), el siguiente capítulo se centra en algunos de los derechos y aspectos sobre los que puede ser de especial interés recibir orientaciones. Además, este capítulo y su análisis dependen de que el tratamiento con la TRF en cuestión haya cumplido los requisitos legales descritos en el capítulo anterior.

84. Dada la naturaleza del tratamiento de datos personales a través de la TRF (tratamiento de categorías especiales de datos personales a menudo sin ninguna interacción aparente con el interesado), el responsable del tratamiento debe considerar detenidamente cómo cumplir (o si puede) los requisitos de la DAP antes de iniciar cualquier tratamiento de la TRF. En particular, analizando detenidamente:

- quiénes son los interesados (a menudo, más personas aparte del destinatario o destinatarios principales a efectos del tratamiento),
- el modo en que se informa a los interesados sobre el tratamiento por TRF (véase la sección 3.2.4.1),
- el modo en que los interesados pueden ejercer sus derechos (en este caso, tanto los derechos de información como los derechos de acceso, así como los derechos de rectificación o limitación, pueden ser especialmente difíciles de preservar en caso de que se utilice la TRF para todas las verificaciones, salvo la verificación individual en contacto directo con el interesado).

3.2.4.1 Dar a conocer los derechos y la información a los interesados de forma concisa, inteligible y fácilmente accesible

85. La TRF plantea dificultades a la hora de garantizar que los interesados sean conscientes de que sus datos biométricos están siendo tratados. Resulta especialmente difícil si una FCS está analizando a través de la TRF material de vídeo procedente de un tercero o que le ha sido facilitado por este, ya que hay pocas posibilidades, y la mayoría de las veces ninguna, de que la FCS notifique la recogida al

[57] Véanse, por ejemplo, las Directrices 1/2022 del CEPD sobre el ejercicio del derecho de acceso, y las Directrices 3/2019 del CEPD sobre el tratamiento de datos personales mediante dispositivos de vídeo.
[58] WP 258, Dictamen sobre algunas cuestiones clave de la DAP (UE 2016/680).

interesado en el momento en que se produce (por ejemplo, mediante un cartel *in situ).* Todo material de vídeo que no sea pertinente para la investigación (o la finalidad del tratamiento) debe ser eliminado o anonimizado en todo caso (por ejemplo, mediante difuminación sin posibilidad de retrocesión para recuperar los datos) antes de desplegar cualquier tratamiento de datos biométricos, a fin de evitar el riesgo de incumplir el principio de minimización del artículo 4, apartado 1, letra e), de la DAP y las obligaciones de información del artículo 13, apartado 2, de la DAP. Incumbe al responsable del tratamiento evaluar qué información sería importante para el interesado a la hora de ejercer sus derechos y garantizar que se facilite la información necesaria. El ejercicio efectivo de los derechos del interesado depende de que el responsable del tratamiento cumpla sus obligaciones de información.

86. El artículo 13, apartado 1, de la DAP establece qué información mínima debe facilitarse al interesado con carácter general. Esta información puede facilitarse a través del sitio web del responsable del tratamiento, en formato impreso (por ejemplo, un folleto disponible previa solicitud) o en otras fuentes de fácil acceso para el interesado. En cualquier caso, el responsable del tratamiento debe asegurarse de que la información se facilita de manera efectiva, como mínimo, en relación con los siguientes elementos:

- la identidad y datos de contacto del responsable del tratamiento, incluido el responsable de la protección de datos;
- la finalidad del tratamiento y que se trata de un tratamiento a través de TRF;
- el derecho a presentar una reclamación ante una autoridad de control y los datos de contacto de dicha autoridad;
- el derecho a solicitar el acceso a los datos personales, así como su rectificación o supresión, y la restricción del tratamiento de los datos personales.

87. Además, en casos específicos definidos en la legislación nacional que deben ser conformes con el artículo 13, apartado 2, de la DAP[59], como por ejemplo el tratamiento de la TRF, debe facilitarse directamente al interesado la siguiente información:

- la base jurídica para el tratamiento;
- información sobre dónde se recogieron los datos personales sin el conocimiento del interesado;
- el período durante el cual se almacenarán los datos personales o, cuando ello no sea posible, los criterios utilizados para determinar dicho período;
- si procede, las categorías de destinatarios de los datos personales (incluidos terceros países u organizaciones internacionales).

88. Mientras que el artículo 13, apartado 1, de la DAP se refiere a información general puesta a disposición del público, el artículo 13, apartado 2, de la DAP se refiere a la información adicional que debe facilitarse al interesado en casos concretos, por ejemplo, cuando los datos se recogen directamente del interesado o indirectamente sin el conocimiento del interesado[60]. No existe una definición clara de lo que se entiende por «casos concretos» en el artículo 13, apartado 2, de la DAP. Sin embargo, alude a situaciones en las que los interesados deben tener conocimiento del tratamiento que se refiere específicamente a ellos y recibir la información adecuada para ejercer efectivamente sus derechos. El

[59] Por ejemplo, el artículo 56, apartado 1, de la Ley Federal alemana de protección de datos, que establece, entre otras cosas, qué información debe facilitarse a los interesados en las operaciones cubiertas.
[60] Dictamen del WP 258 sobre algunas cuestiones clave de la DAP (UE 2016/680), pp. 17-18.

CEPD considera que, al valorar si existe un «caso concreto», deben tenerse en cuenta varios factores, en particular si los datos personales se recogen sin el conocimiento del interesado, ya que esta sería la única manera de permitir a los interesados ejercer efectivamente sus derechos. Otros ejemplos de «casos concretos» podrían ser aquellos en los que los datos personales se tratan posteriormente como objeto de un procedimiento de cooperación penal internacional o en la situación de que los datos personales se tratan en el marco de operaciones encubiertas de conformidad con la legislación nacional. Además, del considerando 38 de la DAP se desprende que, en caso de que la toma de decisiones se base únicamente en la TRF, los interesados deben ser informados sobre las características de la toma de decisiones automatizada. Esto también indicaría que se trata de un caso específico en el que debe facilitarse información adicional al interesado de conformidad con el artículo 13, apartado 2, de la DAP[61].

89. Por último, cabe señalar que, de conformidad con el artículo 13, apartado 3, de la DAP, los Estados miembros pueden adoptar medidas legislativas que limiten la obligación de proporcionar información en casos específicos para determinados objetivos. Esto es así en tanto en cuanto dicha medida constituya una medida necesaria y proporcionada en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos del interesado.

3.2.4.2 Derecho de acceso

90. En general, el interesado tiene derecho a recibir una confirmación positiva o negativa de cualquier tratamiento de sus datos personales y, si la respuesta es positiva, el acceso a los datos personales como tales, más la información adicional enumerada en el artículo 14 de la DAP. Para la TRF, cuando los datos biométricos se almacenan y se vinculan a una identidad también mediante datos alfanuméricos, esto debería permitir a la autoridad competente confirmar una solicitud de acceso basándose en una búsqueda por esos datos alfanuméricos y sin poner en marcha ningún tratamiento posterior de datos biométricos de otros (es decir, buscando con la TRF en una base de datos). Debe respetarse el principio de minimización de los datos, y no deben almacenarse más datos de los necesarios para la finalidad del tratamiento.

3.2.4.3 Derecho a la rectificación de los datos personales

91. Dado que la TRF no ofrece una precisión absoluta, es de especial importancia que los responsables del tratamiento estén atentos a las solicitudes de rectificación de datos personales. También puede darse el caso de que un interesado, basándose en la TRF, haya sido incluido en una categoría incorrecta, por ejemplo, en la categoría de sospechosos, basándose en una presunción inicial sobre los hechos registrados en una grabación de vídeo. Los riesgos para los interesados son especialmente graves si esos datos inexactos se almacenan en una base de datos policial y/o se comparten con otras entidades. El responsable del tratamiento debe corregir en consecuencia los datos almacenados y los sistemas de TRF (véase el considerando 47 de la DAP).

3.2.4.4 Derecho de supresión

92. En la mayoría de los casos (salvo que se utilice para la verificación/autenticación individual) la TRF implica el tratamiento de un gran número de datos biométricos de los interesados. Por lo tanto, es importante que el responsable del tratamiento considere de antemano dónde se encuentran los límites de su finalidad y necesidad, de modo que se pueda tramitar sin demora indebida cualquier solicitud de supresión de conformidad con el artículo 16 de la DAP (ya que el responsable del

[61] Obsérvese bien la diferencia entre «poner a disposición del interesado» en el artículo 13, apartado 1, de la DAP y «proporcionar al interesado» en el artículo 13, apartado 2, de la DAP. En el artículo 13, apartado 2, de la DAP, el responsable del tratamiento debe garantizar que la información llegue al interesado cuando la información publicada en un sitio web no sea suficiente.

tratamiento debe suprimir, en particular, los datos personales que se tratan más allá de lo permitido por la legislación aplicable con arreglo a los artículos 4, 8 y 10 de la DAP).

3.2.4.5 Derecho de limitación

93. En caso de que el interesado impugne la exactitud de los datos y no pueda determinarse la exactitud de estos (o cuando los datos personales deban conservarse a efectos de futuras pruebas), el responsable del tratamiento tiene la obligación de limitar los datos personales de dicho interesado de conformidad con el artículo 16 de la DAP. Esto adquiere especial importancia cuando se trata de la tecnología de reconocimiento facial (basada en algoritmos y que, por tanto, nunca muestra un resultado definitivo) en situaciones en las que se recogen grandes cantidades de datos y la precisión y la calidad de la identificación pueden variar. Con material de vídeo de mala calidad (por ejemplo, de la escena de un crimen) aumenta el riesgo de falsos positivos. Además, si las imágenes faciales de una lista de observación no se actualizan periódicamente, también aumentará el riesgo de falsos positivos o falsos negativos. En casos específicos, cuando los datos no puedan suprimirse debido a que existen motivos razonables para creer que la supresión podría afectar a los intereses legítimos del interesado, los datos deben limitarse y tratarse únicamente para los fines que impidieron su supresión (véase el considerando 47 de la DAP).

3.2.4.6 Limitaciones legítimas de los derechos del interesado

94. En lo que respecta a las obligaciones de información del responsable del tratamiento y al derecho de acceso de los interesados, las limitaciones solo se permiten en la medida en que se establezcan en la legislación que, a su vez, debe constituir una medida necesaria y proporcionada en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física de que se trate (véanse los artículos 13, apartados 3 y 4; 15 y 16, apartado 4, de la DAP). Cuando la TRF se utiliza con fines de aplicación de la ley, es lógico que se haga en circunstancias en las que sería perjudicial para el fin perseguido informar al interesado o permitirle el acceso a los datos. Sería el caso, por ejemplo, de la investigación policial de un delito o a fin de proteger la seguridad nacional o la seguridad pública.

95. El derecho de acceso no significa automáticamente el acceso a toda la información, por ejemplo, en un proceso penal en el que se recojan datos personales. Un ejemplo válido de cuándo se pueden permitir limitaciones a este derecho podría ser durante el curso de una investigación penal.

3.2.4.7 Ejercicio de los derechos a través de la autoridad de control

96. En los casos en que existan limitaciones legítimas del ejercicio de los derechos con arreglo al capítulo III de la DAP, el interesado puede solicitar a la autoridad de protección de datos que ejerza sus derechos en su nombre comprobando la legalidad del tratamiento del responsable del tratamiento. Corresponde al responsable del tratamiento informar al interesado de la posibilidad de ejercer sus derechos de esta forma [véanse los artículos 17 y 46, apartado 1, letra g) de la DAP]. En el caso de la TRF, esto significa que el responsable del tratamiento debe garantizar que se aplican las medidas adecuadas para poder tramitar dicha solicitud, por ejemplo, permitir la búsqueda de material grabado, siempre que el interesado proporcione información suficiente para localizar sus datos personales.

3.2.5 Otros requisitos legales y garantías

3.2.5.1 Artículo 27: Evaluación de impacto relativa a la protección de datos

97. Antes de utilizar la TRF es requisito obligatorio una evaluación de impacto relativa a la protección de datos (EIPD), ya que es probable que el tipo de tratamiento, en particular mediante el uso de nuevas tecnologías, y teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, entrañe un alto riesgo para los derechos y libertades de las personas físicas. Dado que el uso de la TRF implica un tratamiento automático sistemático de categorías especiales de datos, cabe suponer que

en tales casos el responsable del tratamiento está obligado, por regla general, a llevar a cabo una EIPD. La evaluación de impacto relativa a la protección de datos debe contener, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en relación con los fines, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas previstas para abordar dichos riesgos, las garantías, las medidas de seguridad y los mecanismos para garantizar la protección de los datos personales y demostrar el cumplimiento. El CEPD recomienda hacer públicos los resultados de dichas evaluaciones, o al menos las principales constataciones y conclusiones de la evaluación de impacto, como medida de fomento de la confianza y la transparencia[62].

3.2.5.2 Artículo 28: Consulta previa a la autoridad de control

98. De conformidad con el artículo 28 de la DAP, el responsable o el encargado del tratamiento debe consultar a la autoridad de control antes del tratamiento cuando: a) una evaluación de impacto relativa a la protección de datos indique que el tratamiento generará un alto riesgo si el responsable del tratamiento no toma medidas para mitigarlo, o b) el tipo de tratamiento, en particular si se utilizan nuevas tecnologías, mecanismos o procedimientos, implique un alto riesgo para los derechos y libertades de los interesados. Como ya se ha explicado en la sección 2.3. de las presentes directrices, el CEPD considera que la mayoría de los casos de implantación y uso de la TRF entrañan un alto riesgo intrínseco para los derechos y libertades de los interesados. Por lo tanto, además de la EIPD, la autoridad que despliega la TRF debe consultar a la autoridad de control competente antes de poner en funcionamiento el sistema.

3.2.5.3 Artículo 29: Seguridad del tratamiento

99. La naturaleza única de los datos biométricos hace imposible que un interesado los modifique, en caso de que se vea comprometido, por ejemplo, como resultado de una violación de la seguridad de los datos. Por consiguiente, la autoridad competente que aplique o utilice la TRF debe prestar especial atención a la seguridad del tratamiento, de conformidad con el artículo 29 de la DAP. En particular, las autoridades policiales deben velar por que el sistema cumpla las normas pertinentes, y han de adoptar medidas de protección de la plantilla biométrica[63]. Esta obligación es aún más pertinente si la autoridad policial recurre a los servicios de un tercero (encargado del tratamiento de datos).

3.2.5.4 Artículo 20: Protección de datos desde el diseño y por defecto

100. La protección de datos desde el diseño y por defecto, de conformidad con el artículo 20 de la DAP, tiene por objeto garantizar que los principios y garantías de la protección de datos, como la minimización de datos y la limitación del almacenamiento, se integren en la tecnología a través de medidas técnicas y organizativas adecuadas, como la seudonimización, incluso antes del inicio del tratamiento de los datos personales, y se apliquen a lo largo de todo su ciclo de vida. Dado el alto riesgo inherente para los derechos y libertades de las personas físicas, la elección de tales medidas no debe depender únicamente de consideraciones económicas[64], sino que se ha de hacer lo posible por implementar las tecnologías de protección de datos más avanzadas. En la misma línea, si una autoridad de seguridad tiene la intención de aplicar y utilizar la TRF de proveedores externos, debe garantizar (por ejemplo, mediante el procedimiento de contratación) que solo se implanta una TRF basada en los

[62] Para más información, véase WP 248 rev.01, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo».
[63] Véase, por ejemplo: ISO/IEC 24745 Seguridad de la información, ciberseguridad y protección de la privacidad – Protección de la información biométrica.
[64] Véase el considerando 53 de la DAP.

principios de protección de datos desde el diseño y por defecto[65]. Esto también implica que la transparencia sobre el funcionamiento de la TRF no se vea limitada por alegaciones de secretos comerciales o derechos de propiedad intelectual.

3.2.5.5 Artículo 25: Registro de operaciones

101. La DAP establece diferentes métodos para que el responsable o el encargado del tratamiento acrediten la licitud del tratamiento y garanticen la integridad y la seguridad de los datos. A este respecto, los registros del sistema son una herramienta muy útil y una importante garantía para la verificación de la licitud del tratamiento, tanto en el ámbito interno (es decir, el autocontrol) como por parte de las autoridades de control externas, en particular las autoridades de protección de datos. De conformidad con el artículo 25 de la DAP, deben conservarse al menos los registros correspondientes a las siguientes operaciones de tratamiento en sistemas de tratamiento automatizados: recogida, alteración, consulta, comunicación (incluidas las transferencias), combinación y supresión. Además, los registros de consulta y comunicación deben permitir determinar la justificación, la fecha y la hora de tales operaciones y, en la medida de lo posible, el nombre de la persona que consultó o comunicó datos personales, así como la identidad de los destinatarios de dichos datos personales. Además, en el contexto de los sistemas de reconocimiento facial, se recomienda registrar las siguientes operaciones de tratamiento adicionales (algunas de ellas no previstas en el artículo 25 de la DAP):

- Modificaciones de la base de datos de referencia (adición, supresión o actualización). El registro debe conservar una copia de la imagen (añadida, suprimida o actualizada), cuando de otro modo no sea posible verificar la licitud o el resultado de las operaciones de tratamiento.

- Intentos de identificación o verificación, incluido el resultado y la puntuación de confianza. Debe aplicarse el principio estricto de minimización, de modo que solo se conserve en los registros el identificador de la imagen de la base de datos de referencia, en lugar de almacenar la imagen de referencia. Debe evitarse el registro de los datos biométricos de entrada, a menos que sea necesario (por ejemplo, solo en los casos de coincidencia)

- El ID del usuario que solicitó el intento de identificación o verificación.

- Los datos personales almacenados en los registros de los sistemas están sujetos a estrictas limitaciones de finalidad (por ejemplo, auditorías) y no deben utilizarse para otros fines (por ejemplo, para poder seguir realizando el reconocimiento/verificación, incluida una imagen que se ha eliminado de las bases de datos de referencia). Deben aplicarse medidas de seguridad para garantizar la integridad de los registros, siendo muy recomendables los sistemas de supervisión automática para detectar el uso indebido de los registros. Para los registros de la base de datos de referencia, las medidas de seguridad deben ser equivalentes a la base de datos de referencia, en caso de almacenamiento de imágenes faciales. Asimismo, deben implantarse procesos automáticos que garanticen el cumplimiento del periodo de conservación de los datos de los registros.

3.2.5.6 Artículo 4, apartado 4: Responsabilidad

102. El responsable del tratamiento debe poder demostrar la conformidad del tratamiento con los principios del artículo 4, apartados 1 a 3: véase el artículo 4, apartado 4, de la DAP. A este respecto, es esencial una documentación sistemática y actualizada del sistema (incluidas las actualizaciones, las

[65] Para más información, véanse las Directrices del CEPD sobre la protección de datos desde el diseño y por defecto, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

mejoras y el entrenamiento algorítmico), las medidas técnicas y organizativas (incluida la supervisión del rendimiento del sistema y la posible intervención humana) y el tratamiento de los datos personales. Para demostrar la licitud del tratamiento, es especialmente importante el registro con arreglo al artículo 25 de la DAP (véase la sección 3.2.5.5). El principio de rendición de cuentas no solo se refiere al sistema y al tratamiento, sino también a la documentación de las garantías procesales, como las evaluaciones de la necesidad y la proporcionalidad, las EIPD y las consultas internas (por ejemplo, la aprobación por la dirección del proyecto o las decisiones internas sobre los valores de puntuación de confianza) y las consultas externas (por ejemplo, DPA). El Anexo II incluye una serie de elementos a este respecto.

3.2.5.7 Artículo 47: Supervisión efectiva

103. La supervisión efectiva por parte de las autoridades competentes de protección de datos es una de las principales garantías para los derechos y libertades fundamentales de las personas afectadas por el uso de la TRF. Al mismo tiempo, para que puedan desempeñar eficazmente sus funciones y ejercer sus competencias, se ha de proporcionar a cada autoridad de protección de datos los recursos humanos, técnicos y financieros, los locales y las infraestructuras necesarios[66]. Aún más importante que el número de trabajadores disponibles son las competencias de los expertos, que deben abarcar un amplio abanico de temas, desde las investigaciones penales y la cooperación policial hasta el análisis de macrodatos y la inteligencia artificial. Por lo tanto, los Estados miembros deben garantizar que los recursos de las autoridades de control sean adecuados y suficientes para que puedan cumplir su función de proteger los derechos de los interesados y vigilar de cerca cualquier incidencia a este respecto.[67]

4 CONCLUSIÓN

104. El uso de tecnologías de reconocimiento facial está intrínsecamente vinculado al tratamiento de cantidades significativas de datos personales, incluidas categorías especiales de datos. El rostro y, en general, los datos biométricos están vinculados de forma permanente e irrevocable a la identidad de una persona. Por lo tanto, el uso del reconocimiento facial tiene un impacto directo o indirecto en una serie de derechos y libertades fundamentales consagrados en la Carta de los Derechos Fundamentales de la UE que pueden ir más allá de la privacidad y la protección de datos, como la dignidad humana, la libertad de circulación, la libertad de reunión, etc. Esto es especialmente relevante en el ámbito de la aplicación de la ley y la justicia penal.

105. El CEPD comprende la necesidad de que las fuerzas de seguridad dispongan de las mejores herramientas para identificar a los autores de actos terroristas y otros delitos graves. No obstante, estos instrumentos deben utilizarse respetando estrictamente el marco jurídico aplicable y siempre y cuando se cumplan los requisitos de necesidad y proporcionalidad de conformidad con el artículo 52, apartado 1, de la Carta. Además, aunque las tecnologías modernas pueden formar parte de la solución, no son en absoluto una fórmula mágica.

[66] Véase la Comunicación de la Comisión «Primer informe sobre la aplicación y el funcionamiento de la Directiva (UE) 2016/680 sobre protección de datos en el ámbito penal ("DAP")», COM(2022) 364 final, p. 3.4.1.
[67] Véase la contribución del CEPD a la evaluación de la Comisión Europea de la DAP con arreglo al artículo 62, de 14 de diciembre de 2021, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

106. Existen algunos casos de uso de tecnologías de reconocimiento facial que plantean riesgos inaceptablemente elevados para las personas y para la sociedad («líneas rojas»). Por estas razones, el CEPD y el SEPD han pedido su prohibición general[68].

107. En particular, la identificación biométrica a distancia de personas en espacios de acceso público plantea un alto riesgo de intrusión en la vida privada de los individuos y no tiene cabida en una sociedad democrática, ya que, por su naturaleza, implica una vigilancia masiva. En la misma línea, el CEPD considera que son incompatibles con la Carta los sistemas de reconocimiento facial basados en la IA que clasifican a las personas en grupos, partiendo de sus datos biométricos, por razón de su origen étnico, género u orientación política o sexual. Además, el CEPD está convencido de que el uso del reconocimiento facial o de tecnologías similares para inferir las emociones de una persona física es altamente indeseable y debe prohibirse, posiblemente con algunas excepciones debidamente justificadas. Asimismo, el CEPD considera que el tratamiento de datos personales en un contexto de aplicación de la ley que dependa de una base de datos alimentada con la recogida de datos personales a gran escala y de forma indiscriminada, por ejemplo mediante el «arrastre» de fotografías e imágenes faciales accesibles en línea, en particular las que se publican en las redes sociales, no cumpliría, como tal, el requisito de necesidad estricta previsto por el Derecho de la Unión.

5 ANEXOS

Anexo I: Plantilla de apoyo

Anexo II: Guía práctica para la gestión de proyectos de TRF en las FCS

Anexo III: Ejemplos prácticos

[68]Véase el Dictamen conjunto 5/2021 del CEPD-SEPD 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)https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

ANEXO I — MODELO PARA LA DESCRIPCIÓN DE LOS ESCENARIOS

(Con «infoboxes» para los aspectos tratados en cada escenario)

Descripción del tratamiento:

- Descripción del tratamiento, contexto (relación con la delincuencia), finalidad

Fuente de información:

- Tipos de interesados: ☐ todos los ciudadanos ☐ condenados ☐ sospechosos ☐ menores ☐ otros interesados vulnerables
- Origen de la imagen: ☐ espacios públicos ☐ Internet ☐ entidad privada ☐ otras personas ☐ otros .....
- Conexión con la delincuencia: ☐ Temporal directa ☐ Temporal no directa ☐ Geográfica directa ☐ Geográfica no directa ☐ No necesaria
- Modo de captura de información: ☐ a distancia ☐ en una cabina o en un entorno controlado
- Contexto: afecta a otros derechos fundamentales:
  ☐ No
  Sí, a saber: ☐ libertad de reunión
  ☐ libertad de expresión
  ☐ varios:.....
- Posibles fuentes adicionales de información sobre el interesado:
  ☐ documento de identidad ☐uso del teléfono público ☐ matrícula del vehículo
  ☐ otras .....

Base de datos de referencia (con la que se compara la información capturada):

- Especificidad: ☐ bases de datos de uso general ☐ bases de datos específicas de un tipo de delito
- Descripción del origen de los datos de estas bases de datos de referencia (y base jurídica)
- Cambio de finalidad de la base de datos (por ejemplo, la finalidad original era la seguridad de la propiedad privada): ☐ SÍ ☐ NO

Algoritmo:

- Tipo de tratamiento:☐ verificación (autenticación) individual☐ identificación de uno entre muchos
- Consideraciones relativas a la exactitud
- Garantías técnicas

Resultado:

- Impacto ☐ Directo (por ejemplo, el interesado puede ser detenido, interrogado, comportamiento discriminatorio)

  ☐ No directo (se utiliza para modelos estadísticos, ninguna acción legal grave contra los interesados)

- Decisión automatizada: ☐ SÍ ☐ NO
- Duración del almacenamiento

Análisis jurídico:

- Análisis de necesidad y proporcionalidad: finalidad / gravedad del delito / número de personas no implicadas pero afectadas por el tratamiento
- Tipo de información previa al interesado: ☐ Al entrar en la zona específica

  ☐ De forma genérica en el sitio web de la FCS

  ☐ En el sitio web de la FCS con referencia al tratamiento específico

  ☐ Otros .....
- Marco jurídico aplicable:

  ☐ DAP esencialmente trasladada a la legislación nacional

  ☐ Ley nacional genérica sobre el uso de datos biométricos por parte de las FCS

  ☐ Legislación nacional específica sobre este tratamiento (reconocimiento facial) para dicha autoridad competente

  ☐ Legislación nacional específica sobre este tratamiento (decisión automatizada)

Conclusión:

Consideraciones generales sobre la probabilidad de que el tratamiento descrito sea compatible con el Derecho de la Unión (y algunas indicaciones sobre los requisitos jurídicos previos)

ANEXO II — ORIENTACIONES PRÁCTICAS PARA LA GESTIÓN DE PROYECTOS DE TRF EN LAS FCS

El presente anexo ofrece algunas orientaciones prácticas adicionales para los cuerpos y fuerzas de seguridad (FCS) que tengan previsto iniciar un proyecto relacionado con la tecnología de reconocimiento facial (TRF). Proporciona información adicional sobre las medidas organizativas y técnicas que se han de tener en cuenta en la implantación del proyecto, y no debe considerarse una lista exhaustiva de los pasos/medidas que deben adoptarse. También debe verse en conjunción con las [69]Directrices 3/2019 del CEPD sobre el tratamiento de datos personales a través de dispositivos de vídeo y cualquier reglamento de la UE/EEE o directrices del CEPD en relación con el uso de la inteligencia artificial.

El presente anexo ofrece directrices basadas en el supuesto de que las FCS adquieran una TRF (como producto listo para su uso). Si la FCS tiene previsto desarrollar (seguir entrenando) la TRF, debe cumplir requisitos adicionales para seleccionar los conjuntos de datos de entrenamiento, validación y prueba necesarios que se utilizarán durante el desarrollo y las funciones/medidas para el entorno de desarrollo. Del mismo modo, un producto disponible en el mercado puede requerir ajustes adicionales para el uso previsto, y en tal caso deben cumplirse los requisitos mencionados anteriormente para la selección de conjuntos de datos de pruebas, validación y entrenamiento.

El hecho de pertenecer a la misma FCS no proporciona por sí solo pleno acceso a los datos biométricos. Al igual que con cualquier otra categoría de datos personales, los datos biométricos recogidos para una finalidad policial determinada en virtud de una base jurídica específica no pueden utilizarse sin una base jurídica adecuada para fines policiales diferentes [artículo 4, apartado 2, de la Directiva (UE) 2016/680 (DAP)]. Asimismo, el desarrollo o entrenamiento de una herramienta de TRF se considera una finalidad diferente, y es preciso evaluar la necesidad y proporcionalidad del tratamiento de datos biométricos para medir el rendimiento/entrenar la tecnología a fin de evitar el impacto en los interesados en caso de bajo rendimiento, teniendo en cuenta la finalidad inicial del tratamiento.

1. FUNCIONES Y RESPONSABILIDADES

Cuando una FCS emplea la TRF para el desempeño de funciones que entran en el ámbito de aplicación de la DAP (prevención, detección de investigaciones o enjuiciamiento de infracciones penales, etc., de conformidad con el artículo 3 de la DAP), puede considerarse como responsable del tratamiento de la TRF. Sin embargo, las FCS están compuestas por varias unidades o departamentos que pueden intervenir en ese tratamiento, ya sea definiendo el proceso de aplicación de la TRF o aplicándola en la práctica. Debido a las especificidades de esta tecnología, puede ser necesaria la participación de diferentes unidades, ya sea para apoyar en las mediciones de su rendimiento, ya sea para seguir entrenándola.

En un proyecto en el que intervenga la TRF, puede haber diversos actores[70] dentro de las FCS que pueden necesitar participar:

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[70] Las siguientes funciones son ejemplos de los distintos actores y de sus responsabilidades en un proyecto de TRF. Aunque el lenguaje utilizado para describir las funciones en este anexo no es determinante, cada autoridad

- Alta dirección: aprobar el proyecto después de sopesar los riesgos y los posibles beneficios.
- El DPD y/o el departamento jurídico de la FCS: ayudar a evaluar la licitud de la ejecución de un determinado proyecto de TRF; ayudar a realizar la EIPD; garantizar el respeto y el ejercicio de los derechos de los interesados.
- Titular del tratamiento: actuar como unidad específica dentro de la FCS competente para desarrollar el proyecto; decidir los detalles del proyecto de TRF, incluidos los requisitos de rendimiento del sistema; decidir sobre la métrica de imparcialidad adecuada; establecer la puntuación de confianza[71]; establecer umbrales aceptables de sesgo; identificar los riesgos potenciales que el proyecto de TRF entraña para los derechos y libertades de las personas, consultando también al DPD y al Departamento de IA informática y/o Ciencia de Datos (véase más adelante), y exponerlos a la alta dirección. El titular del tratamiento también ha de consultar al gestor de la base de datos de referencia antes de decidir sobre los detalles del proyecto de TRF, para comprender tanto la finalidad de uso de la base de datos de referencia como sus detalles técnicos. En caso de reentrenamiento de una TRF adquirida, el titular del tratamiento también debe encargarse de la selección del conjunto de datos de entrenamiento. Al ser la unidad encargada de desarrollar y decidir los detalles del proyecto, el titular del tratamiento debe encargarse de realizar la EIPD.
- Departamento de IA informática y/o Ciencia de Datos: ayudar a llevar a cabo una EIPD; explicar las métricas disponibles para medir el rendimiento del sistema, la imparcialidad[72] y el sesgo potencial; implantar la tecnología y las garantías técnicas, con el fin de evitar el acceso no autorizado a los datos recogidos, ciberataques, etc. En caso de reentrenamiento de una TRF adquirida, el departamento de IA informática o Ciencia de Datos entrenará el sistema basándose en el conjunto de datos de entrenamiento proporcionado por el titular del tratamiento. También corresponde a este departamento establecer las medidas para mitigar los riesgos identificados conjuntamente por los titulares del tratamiento (por ejemplo, riesgos específicos de la IA, como los ataques a la inferencia de modelos).
- Usuarios finales (como los agentes de policía sobre el terreno o en los laboratorios forenses): llevar a cabo una comparación con la base de datos; revisar críticamente los resultados teniendo en cuenta las pruebas anteriores, y proporcionar información al titular del tratamiento sobre los falsos positivos y los indicios de posible discriminación.
- Gestor de la base de datos de referencia: la unidad específica, dentro de la FCS competente, encargada de acumular y gestionar la base de datos de referencia, es decir, la base de datos con la que se compararán las imágenes, incluida la eliminación de imágenes faciales tras el periodo de conservación definido. Dicha base de datos puede crearse específicamente para el proyecto de TRF o puede existir previamente, si los fines son compatibles. El gestor de la base de datos de referencia se encarga de definir cuándo y en qué circunstancias pueden almacenarse las imágenes faciales, así como de establecer sus requisitos de conservación de datos (en función del tiempo u otros criterios).

de seguridad debe definir y asignar funciones similares en función de su organización. Puede darse el caso de que una unidad acumule más de una función; por ejemplo, el titular del tratamiento y el gestor de la base de datos de referencia, o el titular del tratamiento y el Departamento de IA informática o de Ciencia de Datos (en caso de que la unidad del titular del tratamiento posea todos los conocimientos técnicos necesarios).

[71] La puntuación de confianza es el nivel de confianza de la predicción (coincidencia), en forma de probabilidad. Por ejemplo, comparando dos plantillas existe una confianza del 90 % de que pertenezcan a la misma persona. La puntuación de confianza es diferente del rendimiento de la TRF, aunque afecta a este. Cuanto más elevado sea el umbral de confianza, menos falsos positivos y más falsos negativos se producirán en los resultados de la TRF.

[72] La equidad puede definirse como la ausencia de discriminación injusta e ilícita, como el sesgo de género o de raza.

Dado que la mayoría de los casos de implantación y uso de la TRF entrañan un alto riesgo intrínseco para los derechos y libertades de los interesados, la autoridad de control de la protección de datos también debe participar en la consulta previa que exige el artículo 28 de la DAP.

2. INICIO/ANTES DE ADQUIRIR EL SISTEMA DE TRF

En primer lugar, el titular de tratamiento en una FCS debe tener una comprensión clara del tratamiento o tratamientos para los que se requiere la TRF (el caso o casos de uso) y asegurarse de que existe una base legal para fundamentar el caso de uso previsto. Partiendo de esta premisa, se necesita:

- Describir formalmente el caso de uso. Debe describirse el problema que se trata de resolver y la contribución que ha de hacer la TRF a su solución, así como los aspectos generales del proceso (tarea) en el que se aplicará. A este respecto, las FCS deben documentar al menos[73]:
  - Las categorías de datos personales registrados en el proceso
  - Los objetivos y fines concretos para los que se utilizará la TRF, incluidas las posibles consecuencias para el interesado en caso de coincidencia.
  - Cuándo y cómo se recogerán las imágenes faciales (con información sobre el contexto de esta recogida: en la puerta del aeropuerto, vídeos de cámaras de seguridad fuera de una tienda donde se cometió un delito, etc., y las categorías de interesados cuyos datos biométricos se tratarán).
  - La base de datos con la que se compararán las imágenes (base de datos de referencia), así como información sobre cómo se creó, su tamaño y la calidad de los datos biométricos que contiene.
  - Los actores de la FCS que estarán autorizados a utilizar el sistema de TRF y a adoptar medidas policiales partiendo de él (sus perfiles y derechos de acceso deben ser definidos por el titular del tratamiento).
  - El período de conservación previsto para los datos obtenidos, o el momento que determinará el final de este período (como el cierre o la conclusión del proceso penal de conformidad con el Derecho procesal nacional para el que se hayan recogido inicialmente), así como cualquier acción posterior (supresión de estos datos, anonimización y uso con fines estadísticos o de investigación, etc.).
  - Implantación de registros y accesibilidad de los registros y archivos conservados.
  - Los parámetros de rendimiento (por ejemplo, exactitud, precisión, recuperación, puntuación F1) y sus valores mínimos aceptables.[74]
  - Una estimación del número de personas a las que se aplicará la TRF y en qué periodo de tiempo / ocasión.

[73] El anexo I proporciona una lista de elementos que ayudan al responsable del tratamiento a describir un caso de uso de la TRF.

[74] Existen diferentes parámetros para evaluar el rendimiento de un sistema de TRF. Cada uno ofrece una visión diferente de los resultados del sistema, y su eficacia a la hora de proporcionar una imagen adecuada del buen funcionamiento del sistema de TRF depende del asunto en que se utilice la TRF. Si el objetivo es lograr altos porcentajes de coincidencias correctas de un rostro, podrían utilizarse parámetros como la precisión y el recuerdo. Sin embargo, estos parámetros no miden en qué medida la TRF gestiona ejemplos negativos (cuántas falsas coincidencias realizó el sistema). El titular del tratamiento, apoyado por el Departamento de IA informática y Ciencia de Datos, debe poder establecer los requisitos de rendimiento y expresarlo en el parámetro más adecuado para el caso de uso de la TRF.

- Evaluar la necesidad y la proporcionalidad[75]. El hecho de que esta tecnología exista no debe ser el único motivo para aplicarla. El titular del tratamiento debe evaluar en primer lugar si existe una base jurídica adecuada para el tratamiento previsto. Para ello, es necesario consultar al DPD y al servicio jurídico. El factor que impulse la implantación de la TRF debe ser su necesidad y proporcionalidad como solución para un problema específico de las FCS. Esto debe evaluarse en función de la finalidad/gravedad de la delincuencia y el número de personas no implicadas pero afectadas por el sistema de TRF. A efectos de valorar la licitud debe tenerse en cuenta, como mínimo, lo siguiente: La DAP[76], el RGPD[77] [78], la normativa que exista en materia de IA[79] y todas las directrices de acompañamiento proporcionadas por las autoridades de control de la protección de datos (como las Directrices 3/2019 del CEPD sobre el tratamiento de datos personales mediante dispositivos de vídeo[80]). Estos actos legislativos de la UE deben reflejarse siempre en los requisitos nacionales aplicables, especialmente en el ámbito del Derecho procesal penal. La evaluación de la proporcionalidad ha de identificar los derechos fundamentales de los interesados que pueden verse afectados (aparte de la vida privada y la protección de datos). También debe describir y tener en cuenta cualquier límite (o falta de límites) impuesto al sistema de TRF en el caso de uso. Por ejemplo, si el sistema funcionará de forma continua o temporal y si se limitará a una zona geográfica.
- Realizar una evaluación del impacto relativa a la protección de datos (EIPD)[81]. Debe llevarse a cabo una EIPD, ya que el despliegue de la TRF en el ámbito de la aplicación de la ley tiende a generar un alto riesgo para los derechos y libertades de las personas[82]. La EIPD debe incluir, en particular: una descripción general de las operaciones de tratamiento previstas[83], una evaluación de los

[75] Puede considerarse la posibilidad de adoptar medidas adicionales para tener en cuenta la necesidad en cuanto a la adaptación y el uso del sistema, por lo que la descripción del caso de uso también puede sufrir alguna alteración durante la evaluación de la necesidad y la proporcionalidad.

[76] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

[77] Reglamento (UE) n.º 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.

[78] Cuando un proyecto científico destinado a investigar el uso de la TRF necesite tratar datos personales, pero sin que este tratamiento entre en el ámbito de aplicación del artículo 4, apartado 3, de la DAP, en general será aplicable el RGPD (artículo 9, apartado 2, de la DAP). En el caso de proyectos piloto que hayan de preceder a operaciones policiales, seguirá siendo aplicable la DAP.

[79] Por ejemplo, existe una 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, pero aún no ha sido aprobado.

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Para más orientaciones sobre las EIPD, véase: Directrices 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 2016/679, WP 248 rev.01, disponibles en: https://ec.europa.eu/newsroom/article29/items/611236 y el conjunto de herramientas de rendición de cuentas del SEPD sobre el terreno, parte II, disponible en: https://edps.europa.eu/node/4582_en

[82] La TRF, dependiendo del caso de uso, puede entrar en el ámbito de los siguientes criterios que motivan el tratamiento de alto riesgo (de las Directrices sobre la EIPD, WP 248 rev.01): observación sistemática, tratamiento de datos a gran escala, asociación o combinación de conjuntos de datos, uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas.

[83] La descripción del tratamiento, así como la evaluación de la necesidad y la proporcionalidad, ya descritas en los pasos anteriores, también forman parte de la EIPD, además de la evaluación de riesgos. En caso necesario, en la evaluación del impacto sobre la protección de datos se facilitará una descripción más detallada de los flujos de datos personales.

riesgos para los derechos y libertades de los interesados[84], las medidas previstas para mitigar dichos riesgos, las garantías, las medidas de seguridad y los mecanismos para asegurar la protección de los datos personales y demostrar el cumplimiento. La EIPD es un proceso continuo, por lo se le ha de añadir cualquier nuevo elemento del tratamiento y debe actualizarse en cada fase del proyecto.

- Obtener la aprobación de la alta dirección exponiéndole los riesgos que existen para los derechos y libertades de los interesados (derivados del caso de uso y de la tecnología) y los planes para mitigarlos.

3. DURANTE LA CONTRATACIÓN PÚBLICA Y ANTES DE IMPLANTAR LA TRF

- Decidir los criterios para seleccionar la TRF (algoritmo). El titular del tratamiento debe decidir los criterios para seleccionar un algoritmo, con la ayuda del departamento de IA Informática y/o Ciencia de Datos. En la práctica, estas medidas incluirán los parámetros de equidad y rendimiento elegidos en la descripción del caso de uso. Estos criterios también deben incluir información relativa a los datos con los que se entrenó el algoritmo. El conjunto de entrenamiento, prueba y validación debe incluir muestras suficientes de todas las características de los interesados que se someterán a la TRF (considérese, por ejemplo, la edad, el sexo y la raza) para reducir el sesgo. El proveedor de la TRF debe proporcionar información y parámetros sobre los conjuntos de datos de entrenamiento, prueba y validación de la TRF, y describir las medidas adoptadas para medir y mitigar la posible discriminación ilegal y el sesgo. El titular del tratamiento, en la medida de lo posible, debe comprobar si existía una base jurídica para que el proveedor utilizara este conjunto de datos a efectos del entrenamiento de los algoritmos (sobre la base de la información facilitada por el proveedor). Asimismo, el titular del tratamiento debe garantizar que el proveedor de la TRF aplique normas de seguridad relacionadas con los datos biométricos, como la norma ISO/IEC 24745, que proporciona orientaciones para la protección de la información biométrica con arreglo a diversos requisitos de confidencialidad, integridad y renovabilidad/revocabilidad durante el almacenamiento y la transmisión, así como requisitos y directrices para la gestión y el tratamiento seguros y respetuosos con la privacidad de la información biométrica.

- Reentrenar el algoritmo (si es necesario). El titular del tratamiento debe garantizar que los servicios contratados incluyan también el ajuste del sistema de TRF para lograr una mayor precisión antes de comenzar a utilizarlo. En caso de que sea necesario un entrenamiento adicional del sistema de TRF adquirido para cumplir los parámetros de exactitud, el titular del tratamiento, además de decidir sobre el reentrenamiento, debe elegir, con la ayuda de IA Informática o del Departamento de Ciencia de Datos, el conjunto de datos adecuado y representativo que se ha de utilizar, y comprobar la legalidad de este uso para los datos.
- Disponer las garantías adecuadas para tratar los riesgos relacionados con la seguridad, los sesgos y el bajo rendimiento. Esto incluye el establecimiento de un proceso para supervisar la TRF durante su utilización (registro y evaluación sobre la precisión y la equidad de los resultados). Además, es preciso asegurarse de que se identifican, miden y mitigan los riesgos que son específicos de algunos sistemas de aprendizaje automático y de TRF (por ejemplo, intoxicación de

[84] El análisis de los riesgos para los interesados debe incluir los riesgos relacionados con el lugar de las imágenes faciales que se van a comparar (local/remoto), los riesgos relacionados con los encargados/subencargados del tratamiento y los riesgos específicos del aprendizaje automático, cuando se aplique (por ejemplo, intoxicación de datos, ejemplos contradictorios).

datos, ejemplos contradictorios, inversión de modelos, inferencia de caja blanca). El responsable del proceso también debe disponer las garantías adecuadas para que se respeten los requisitos de conservación de los datos biométricos incluidos en el conjunto de datos de reentrenamiento.

- Documentar el sistema de TRF. Esto debe incluir una descripción general del sistema de TRF, una descripción detallada de los elementos del sistema de TRF y del proceso para su establecimiento, información detallada sobre el seguimiento, el funcionamiento y el control del sistema de TRF y una descripción detallada de sus riesgos y las medidas para mitigarlos. Esta documentación ha de recoger los principales elementos de la descripción del sistema de TRF de fases anteriores (véase más arriba), si bien se ampliará con información relacionada con la supervisión del rendimiento y la aplicación de cambios en el sistema, incluidas posibles actualizaciones de versión y/o reciclaje.
- Crear manuales de usuario que expliquen la tecnología y los casos de uso. Estos deben explicar con claridad todas las situaciones en que se utilizará la TRF y los requisitos para ello.
- Formar a los usuarios finales en la utilización de la tecnología. Esta formación debe explicar las capacidades y limitaciones de la tecnología, para que los usuarios puedan comprender las circunstancias en las que es necesario aplicarla y los casos en los que puede resultar inexacta. También ha de contribuir a mitigar los riesgos que entraña el hecho de no comprobar/someter a crítica los resultados del algoritmo.
- Consultar a la autoridad de control de la protección de datos, de conformidad con el artículo 28, apartado 1, letra b), de la DAP. Facilitar información de conformidad con el artículo 13 de la DAP, para que los interesados conozcan el tratamiento y sus derechos. Estas comunicaciones deben dirigirse a los interesados en un lenguaje adecuado que les permita comprender el tratamiento y los elementos básicos de la tecnología, incluidas las tasas de exactitud, los conjuntos de datos de entrenamiento y las medidas adoptadas para evitar la discriminación y la baja exactitud del algoritmo.

4. RECOMENDACIONES TRAS LA IMPLANTACIÓN DE LA TRF

- Garantizar la intervención humana y la supervisión de los resultados. No adoptar nunca ninguna medida relativa a una persona basándose únicamente en el resultado de la TRF (esto supondría una infracción del artículo 11 de la DAP: toma de decisiones individuales automatizadas que tengan consecuencias legales u otros efectos similares sobre el interesado). Garantizar que un funcionario de las FCS revise los resultados de la TRF. Garantizar asimismo que los usuarios de las FCS eviten el sesgo de automatización, investigando la información contradictoria y cuestionando de manera crítica los resultados de la tecnología. Para ello, es importante la formación continua y la sensibilización de los usuarios finales, aunque la alta dirección debe garantizar que se dispone de los recursos humanos adecuados para llevar a cabo una supervisión eficaz. Esto implica proporcionar a cada agente tiempo suficiente para cuestionar de manera crítica los resultados de la tecnología. Registrar, medir y evaluar en qué medida la supervisión humana modifica la decisión original de la TRF.
- Supervisar y abordar la desviación del modelo de TRF (degradación del rendimiento) una vez que el modelo esté en producción.
- Establecer un proceso para reevaluar los riesgos y las medidas de seguridad con regularidad y cada vez que se modifique la tecnología o el caso de uso.
- Documentar cualquier cambio en el sistema a lo largo de su ciclo de vida (por ejemplo, actualizaciones, reciclaje profesional).
- Establecer un proceso, así como las capacidades técnicas relacionadas, para abordar las solicitudes de acceso de los interesados. La capacidad técnica para la extracción de datos, en caso de que sea necesario facilitarlos a los interesados, debe estar disponible antes de que se presente cualquier solicitud.

- Comprobar que existen procedimientos para las violaciones de la seguridad de los datos. En caso de que se produzca una violación de la seguridad de los datos personales que implique datos biométricos, es probable que los riesgos sean elevados. En este caso, todos los usuarios implicados deben conocer los procedimientos pertinentes, se debe dar parte inmediatamente al DPD y se debe informar a los interesados.

ANEXO III - EJEMPLOS PRÁCTICOS

Existen múltiples situaciones y finalidades prácticas diferentes para el uso del reconocimiento facial; por ejemplo, en entornos controlados como los pasos fronterizos, la comprobación cruzada con datos de bases de datos policiales, o a partir de datos personales hechos manifiestamente públicos por el interesado, imágenes de cámaras en directo (reconocimiento facial en directo), etc. En consecuencia, los riesgos para la protección de los datos personales y otros derechos y libertades fundamentales varían significativamente entre los distintos casos de uso. Con el fin de facilitar la evaluación de la necesidad y la proporcionalidad que debe preceder a la decisión sobre la posible implantación del reconocimiento facial, las presentes directrices proporcionan una lista no exhaustiva de posibles aplicaciones de la TRF en el ámbito policial.

Los escenarios presentados y evaluados se basan en situaciones **hipotéticas** y tienen por objeto ilustrar determinados usos concretos de la TRF y servir de ayuda para planteamientos concretos, así como establecer un marco general. No aspiran a ser exhaustivos y se entienden sin perjuicio de cualquier procedimiento en curso o futuro emprendido por una autoridad nacional de control en relación con el diseño, la experimentación o la aplicación de tecnologías de reconocimiento facial. La presentación de estos escenarios pretende servir únicamente para ejemplificar la orientación que este documento proporciona a los responsables políticos, legisladores y autoridades policiales a la hora de diseñar y plantear la aplicación de tecnologías de reconocimiento facial, con el fin de garantizar el pleno cumplimiento del acervo de la UE en el ámbito de la protección de datos personales. En este contexto, debe tenerse en cuenta que incluso en situaciones similares de utilización de la TRF, la presencia, o la ausencia, de determinados elementos puede conducir a un resultado diferente de la evaluación de la necesidad y proporcionalidad.

1 ESCENARIO 1:

1.1. Descripción

Un sistema de control fronterizo automatizado que permite un paso fronterizo automatizado mediante la autenticación de la imagen biométrica almacenada en el pasaporte electrónico de los ciudadanos de la UE y otros viajeros que atraviesan el paso fronterizo, y determina que el pasajero es el titular legítimo del documento.

Dicha verificación/autenticación implica únicamente el reconocimiento facial individual y se lleva a cabo en un entorno controlado (por ejemplo, en las puertas electrónicas de los aeropuertos). Los datos biométricos del viajero que atraviesa el paso fronterizo se capturan cuando se le pide explícitamente que mire a la cámara de la puerta electrónica y se comparan con los del documento presentado (pasaporte, tarjeta de identidad, etc.), que se ha expedido conforme a unos requisitos técnicos específicos.

Al mismo tiempo, aunque, en principio, el tratamiento en tales casos queda fuera del ámbito de aplicación de la DAP, el resultado de la verificación también puede utilizarse para cotejar los datos (alfanuméricos) de la persona con las bases de datos policiales con motivo del control fronterizo y, por tanto, puede conllevar acciones con un efectos legales significativos para el interesado, por ejemplo, la detención en virtud de una alerta en el SIS. En circunstancias específicas, los datos biométricos también pueden utilizarse para buscar correspondencias en las bases de datos policiales (en tal caso, se realizaría una identificación de uno entre muchos en esta fase).

El resultado del tratamiento de la imagen biométrica afecta directamente al interesado: solo en caso de verificación satisfactoria se le permite cruzar la frontera. Si la identificación es fallida, los guardias fronterizos deben realizar una segunda comprobación para asegurarse de que el interesado es distinto del que figura en el documento de identificación.

En caso de que se identifique un alerta nacional o del SIS, los guardias de fronteras deben realizar una segunda comprobación y los controles adicionales necesarios y, a continuación, tomar las medidas oportunas, como por ejemplo detener a la persona o informar a las autoridades competentes.

Fuente de información:

- Tipos de interesados: ☒ todas las personas que cruzan las fronteras
- Origen de la imagen: ☒ otros (documento de identidad)
- Conexión con la delincuencia: ☒ No es necesaria
- Modo de captura de la información: ☒ en una cabina o en un entorno controlado
- Contexto: afecta a otros derechos fundamentales: Sí, a saber,el☒ derecho a la libre circulación☒ derecho de asilo

Base de datos de referencia (con la que se compara la información capturada):

- Especificidad: ☒ bases de datos específicas relacionadas con el control de fronteras

Algoritmo:

- Tipo de verificación: ☒ verificación (autenticación) individual

Resultado:

- Impacto ☒ Directo (se permite o se deniega la entrada al interesado)
- Decisión automatizada: ☒ Sí

1.2. Marco jurídico aplicable

Desde 2004, de conformidad con el Reglamento (CE) n.º 2252/2004 del Consejo[85], los pasaportes y otros documentos de viaje expedidos por los Estados miembros deben contener una imagen facial biométrica almacenada en un chip electrónico integrado en el documento.

El Código de fronteras Schengen (CFS)[86] establece los requisitos para el control fronterizo de las personas en las fronteras exteriores. Para los ciudadanos de la UE y otras personas que ejerzan el derecho a la libre circulación en virtud de la legislación de la Unión, los controles mínimos deben consistir en una verificación de sus documentos de viaje, si procede mediante el uso de dispositivos técnicos. El Código de fronteras Schengen se modificó posteriormente con el Reglamento (UE) 2017/2225,[87] que, en particular, ha introducido las definiciones de «puertas automáticas», «sistema automatizado de control fronterizo» y «sistema de autoservicio», así como la posibilidad de tratar datos biométricos para llevar a cabo inspecciones fronterizas.

Por lo tanto, podría suponerse que existe una base jurídica clara y previsible que autoriza esta forma de tratamiento de datos personales. Además, la legislación se ha adoptado a escala de la Unión y es directamente aplicable a los Estados miembros.

[85] REGLAMENTO (CE) n.º 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros.
[86]Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen).
[87]Reglamento (UE) 2017/2225 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se modifica el Reglamento (UE) 2016/399 en lo que respecta a la utilización del Sistema de Entradas y Salidas.

1.3. Necesidad y proporcionalidad: finalidad/gravedad de la delincuencia

La verificación de la identidad de los ciudadanos de la UE en un control fronterizo automatizado, utilizando su imagen biométrica, es un elemento de los controles fronterizos en las fronteras exteriores de la UE. Por consiguiente, está directamente relacionada con la seguridad de las fronteras y sirve a un objetivo de interés general reconocido por la Unión. Además, las puertas ABC ayudan a agilizar el procesamiento de pasajeros y disminuyen el riesgo de errores humanos. Por otro lado, en este escenario el ámbito, el alcance y la intensidad de las interferencias son mucho menores que con otras formas de reconocimiento facial. No obstante, el tratamiento de datos biométricos entraña riesgos adicionales para los interesados, que deben ser abordados y mitigados adecuadamente por la autoridad competente que implanta y gestiona la TRF.

1.4. Conclusión

La verificación de la identidad de los ciudadanos de la UE dentro de un control fronterizo automatizado es una medida necesaria y proporcionada, siempre que existan las garantías adecuadas, en particular la aplicación de los principios de limitación de la finalidad, calidad de los datos, transparencia y un alto nivel de seguridad.

2 ESCENARIO 2

2.1. Descripción

Las FCS establecen un sistema de identificación de las víctimas de sustracción de menores. Un agente de policía autorizado podrá llevar a cabo una comparación de los datos biométricos de un menor sospechoso de ser secuestrado, con una base de datos de víctimas de sustracción de menores, en condiciones estrictas y con el único fin de identificar a los menores que puedan corresponderse con la descripción del menor desaparecido para el que se ha iniciado una investigación y se ha emitido la alerta.

El tratamiento en cuestión sería la comparación del rostro o la imagen de un individuo, que puede corresponder a la descripción de un niño desaparecido, con las imágenes almacenadas en la base de datos. Dicho tratamiento se produciría en casos específicos y no de forma sistemática.

La base de datos con la que se realiza la comparación se nutre de imágenes de niños desaparecidos respecto de los cuales se ha denunciado una sospecha de sustracción de menores o una amenaza para la vida o la integridad física del niño, se ha abierto una investigación penal a cargo de una autoridad judicial, y respecto de los cuales se ha emitido una alerta por sustracción de menores. Los datos se recogen conforme a los procedimientos establecidos por la autoridad policial competente, es decir, los agentes de policía autorizados para llevar a cabo misiones de policía judicial. Las categorías de datos personales registrados son:

- identidad, apodo, alias, filiación, nacionalidad, direcciones, correo electrónico, números de teléfono;
- fecha y lugar de nacimiento;
- datos de los progenitores;
- fotografía con características técnicas que permitan el uso de un dispositivo de reconocimiento facial, y otras fotografías.

Los resultados de la comparación también deben ser revisados y verificados por un funcionario autorizado, con el fin de corroborar las pruebas anteriores con el resultado de la comparación y descartar cualquier posible falso positivo.

Las imágenes y los datos personales de los niños solo pueden conservarse mientras dure la alerta y deben suprimirse inmediatamente después del cierre o la conclusión del proceso penal, de conformidad con el procedimiento nacional para el que se hayan introducido en la base de datos.

Aunque la conservación de los datos biométricos en la base de datos puede prolongarse durante un período de tiempo relativamente largo con arreglo a la legislación nacional, el ejercicio de los derechos de los interesados y, en particular, el derecho de rectificación y supresión ofrece una garantía adicional para limitar la injerencia en el derecho a la protección de los datos personales de los interesados afectados.

Fuente de información:

- Tipos de interesados:☒ menores
- Origen de la imagen☒ otros: no predefinida, posible víctima de sustracción de menores
- Conexión con la delincuencia ☒ Temporal no directa ☒ Geográfica no directa
- Modo de captura de la información: ☒ en una cabina o en un entorno controlado
- Contexto: afecta a otros derechos fundamentales☒ Sí, a saber:☒ varios

Base de datos de referencia (con la que se compara la información capturada):

- Especificidad ☒ base de datos específica

Algoritmo:

- tipo de verificación: ☒ identificación de uno entre muchos

Resultado:

- Impacto ☒ Directo
- Decisión automatizada:☒ NO, revisión obligatoria por un funcionario autorizado

Análisis jurídico:

- Marco jurídico aplicable:☒ Derecho nacional específico para este tratamiento (reconocimiento facial)

2.2. Marco jurídico aplicable

La legislación nacional prevé un marco jurídico específico que establece la base de datos y determina los fines del tratamiento, así como los criterios para rellenar la base de datos, acceder a ella y utilizarla. Las medidas legislativas necesarias para su aplicación también prevén el establecimiento de un periodo de conservación, además de hacer referencia a los principios aplicables de integridad y confidencialidad. Las medidas legislativas también prevén las modalidades de información al interesado y, en este caso, al titular o titulares de la patria potestad, así como el ejercicio de los derechos de los interesados y la posible limitación, si procede. Durante la redacción de la propuesta legislativa correspondiente se ha de consultar a la autoridad nacional de supervisión.

2.3. Necesidad y proporcionalidad: finalidad/gravedad del delito/número de personas no implicadas pero afectadas por el tratamiento

Condiciones y garantías del tratamiento

La comparación del reconocimiento facial solo puede ser llevada a cabo por una persona autorizada como último recurso, a menos que no haya otros medios menos intrusivos disponibles y cuando sea estrictamente necesario, por ejemplo, en caso de duda sobre la autenticidad del documento de identidad de un menor viajero o tras haber revisado las pruebas y materiales anteriores recopilados que indiquen una posible correspondencia con la descripción de un menor desaparecido para el que se está llevando a cabo una investigación penal.

También se ofrece una garantía adicional con la revisión y la verificación obligatorias de la comparación del reconocimiento facial por parte de un funcionario autorizado, con el fin de corroborar las pruebas anteriores con el resultado de la comparación y descartar cualquier posible falso positivo.

Objetivo perseguido

La creación de la base de datos sirve para importantes objetivos de interés público general, en particular la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, así como la protección de los derechos y libertades de terceros. La creación de la base de datos y el tratamiento previsto parecen contribuir a la identificación de los menores víctimas de sustracción y, por lo tanto, pueden considerarse una medida adecuada para apoyar el objetivo legítimo de investigar y enjuiciar dichos delitos.

Finalidad y alimentación de la base de datos

Los fines del tratamiento están claramente definidos por ley, y la base de datos solo se utilizará con el fin de identificar a los menores desaparecidos respecto a los que se haya comunicado una sospecha de sustracción de menores y se haya iniciado una investigación penal bajo la supervisión de una autoridad judicial y para los que se haya emitido una alerta por sustracción de menores. Las condiciones establecidas por la ley para la alimentación de la base de datos tienen por objeto limitar estrictamente el número de interesados y de datos personales que se incluyan en ella. El titular de la patria potestad del menor debe ser informado del tratamiento realizado y de las condiciones para el ejercicio de los derechos del menor en relación con el tratamiento biométrico previsto con fines de identificación, o con los datos personales del menor almacenados en la base de datos.

2.4. Conclusión

Teniendo en cuenta la necesidad y proporcionalidad del tratamiento previsto, así como el interés superior del menor al llevar a cabo dicho tratamiento de datos personales, y siempre que existan garantías suficientes para asegurar, en particular, el ejercicio de los derechos de los interesados, en particular teniendo en cuenta el hecho de que van a ser tratados datos de menores, puede considerarse probable que dicha aplicación del tratamiento de reconocimiento facial sea compatible con el Derecho de la UE.

Además, dado el tipo de tratamiento y la tecnología utilizada, que entraña un alto riesgo para los derechos y libertades del interesado, el CEPD considera que la redacción de una propuesta legislativa que deba adoptar un parlamento nacional o de una medida reglamentaria basada en dicha legislación, que se refiera al tratamiento previsto, debe incluir una consulta previa de la autoridad de control a fin de garantizar la coherencia y el cumplimiento de la legislación aplicable (véase el artículo 28, apartado 2, de la DAP).

3 ESCENARIO 3

3.1. Descripción

En el curso de las intervenciones policiales en los disturbios y de las investigaciones posteriores, se ha identificado a varias personas como sospechosas, por ejemplo, mediante investigaciones previas en las que se ha recurrido a la cobertura de cámaras de videovigilancia o a testigos. Las imágenes de estos sospechosos se comparan con las de personas que fueron grabadas por cámaras de videovigilancia o dispositivos móviles en el lugar del delito o en las zonas circundantes.

Con el fin de obtener pruebas más detalladas sobre las personas sospechosas de haber participado en disturbios en torno a una manifestación, la policía crea una base de datos consistente en imágenes con conexión espacial y temporal poco clara con los disturbios. La base de datos incluye grabaciones privadas subidas a la policía por los ciudadanos, material de los circuitos cerrados de televisión de los transportes públicos, material de videovigilancia perteneciente a la policía y material publicado por los medios de comunicación sin ninguna limitación o garantía específica. El registro de un comportamiento delictivo grave no es un requisito previo para la inclusión de los archivos en la base de datos. Por lo tanto, en la base de datos se incluye a personas no implicadas en los disturbios (un porcentaje significativo de la población local que pasaba por allí en el momento de la manifestación o que participó en la manifestación pero no en los disturbios). Esto equivale a miles de archivos de vídeo e imagen.

Utilizando un software de reconocimiento facial, todos los rostros que aparecen en dichos archivos se asignan a identidades personales únicas. A continuación, se comparan automáticamente los rostros de los sospechosos individuales con estos identificadores de cara. La base de datos que contiene todas las plantillas biométricas de los miles de archivos de vídeo e imágenes se almacena hasta que concluyan todas las investigaciones posibles. Las coincidencias positivas son tratadas por los funcionarios responsables, que deciden qué medidas adoptar. Esto puede incluir atribuir el archivo encontrado en la base de datos al expediente penal de la persona afectada, así como otras medidas, como el interrogatorio o la detención de dicha persona.

La legislación nacional contiene una disposición genérica según la cual el tratamiento de datos biométricos con el fin de identificar de manera unívoca a una persona física es admisible si es estrictamente necesario y está sujeto a las garantías adecuadas para los derechos y libertades de la persona afectada.

Fuente de información:

- Tipos de interesados: ☒ todas las personas
- Origen de la imagen: ☒ espacios de acceso público ☒ entidad privada ☒ otros particulares ☒ otros: medios de comunicación
- Conexión con la delincuencia:☒ Sin necesidad de una conexión geográfica o temporal directa
- Modo de captura de la información: ☒ a distancia
- Contexto: afecta a otros derechos fundamentales: Sí, a saber,☒ la libertad de reunión
- Fuentes adicionales de información disponibles sobre el interesado:
  ☒ otros: no se excluyen (como el uso de cajeros automáticos o la visita a comercios), ya que no puede ejercerse ningún control sobre los motivos de las imágenes

Base de datos de referencia (con la que se compara la información capturada):

- Especificidad: ☒ bases de datos específicas relacionadas con el ámbito de la delincuencia

Algoritmo:

- Tipo de tratamiento: ☒ Identificación de uno entre muchos

Resultado:

- Impacto: ☒ Directo (por ejemplo, el interesado puede ser detenido o interrogado)
- Decisión automatizada: ☒ NO
- Duración del almacenamiento: hasta que finalicen todas las investigaciones posibles

Análisis jurídico:

- Tipo de información previa al interesado: ☒ Con carácter general, en el sitio web de la FCS
- Marco jurídico aplicable : ☒ la DAP, esencialmente trasladada a una ley nacional ☒ Ley nacional genérica sobre el uso de datos biométricos por las FCS

3.2. Marco jurídico aplicable

Como se ha expuesto anteriormente, las bases jurídicas que se limitan a repetir la cláusula general del artículo 10 de la DAP no son suficientemente claras en sus términos para ofrecer a los particulares una indicación adecuada de las condiciones y circunstancias en las que las FCS están facultados para utilizar grabaciones de CCTV de espacios públicos a fin de crear una plantilla biométrica de su rostro y compararla con bases de datos policiales, otras grabaciones de CCTV o privadas disponibles, etc. Por lo tanto, el marco jurídico establecido en este escenario no cumple los requisitos mínimos para servir de base jurídica.

3.3. Necesidad y proporcionalidad

En este ejemplo, el tratamiento suscita diversas inquietudes en cuanto a los principios de necesidad y proporcionalidad, por varias razones:

Las personas no son sospechosas de un delito grave. La visualización de un comportamiento delictivo grave no es un requisito previo para el uso de los archivos en la base de datos que contiene el material de la imagen. Además, no se requiere una conexión temporal y geográfica directa con el delito para el uso de los archivos en la base de datos. Esto da lugar a que un porcentaje significativo de la población local se halle almacenada en una base de datos biométrica, potencialmente durante varios años, hasta que concluyan todas las investigaciones.

La base de datos de la escena del crimen no se limita a las imágenes que cumplen los requisitos de proporcionalidad, lo que lleva a comparar una cantidad ilimitada de imágenes. Esto contradice el principio de minimización de los datos. Una menor cantidad de imágenes también permitiría considerar medios no algorítmicos y menos intrusivos, por ejemplo, fisonomistas.[88]

Dado que el ejemplo se extrae del entorno de una protesta, también es probable que las imágenes revelen las opiniones políticas de los participantes en la manifestación, lo que la convierte en la segunda categoría especial de datos posiblemente afectada en este escenario. En este escenario, no está claro cómo puede impedirse la recogida de estos datos y con qué garantías. Además, cuando los interesados se enteran de que su participación en una manifestación ha dado lugar a su inclusión en

[88] Personas con una capacidad extraordinaria de reconocimiento facial. Véase también: Face Recognition by Metropolitan Police Super-Recognisers, 2016 de febrero de 26, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

una base de datos biométricos de la policía, ello puede tener graves efectos disuasorios para su futuro ejercicio del derecho de reunión.

Las plantillas biométricas de la base de datos también pueden compararse entre sí. Esto permite a la policía no solo buscar una persona concreta en todo su material, sino también volver a crear el patrón de comportamiento de una persona a lo largo de un período de varios días. También puede recabar información adicional sobre las personas, como los contactos sociales y la participación política.

La interferencia se intensifica aún más por el hecho de que los datos se procesan sin el conocimiento de los interesados.

Teniendo en cuenta que las fotografías y vídeos son grabados en todo momento por personas, y que incluso la omnipresente cobertura de CCTV puede analizarse de forma biométrica, esto puede generar graves efectos disuasorios.

Otro motivo de preocupación es el uso generalizado de fotografías y vídeos privados, incluido un posible uso indebido, como la calumnia. Dado que el uso indebido, como la calumnia, es un riesgo también inherente a los procedimientos penales en general, el riesgo es considerablemente mayor en cuanto a la posibilidad de tratar grandes cantidades de datos y afectar a un elevado número de personas, ya que la gente podría subir también material relativo a una persona o grupo de personas con las que no se simpatice. Las solicitudes de la policía de cargar fotografías y vídeos posiblemente den lugar a umbrales muy bajos para que las personas proporcionen material, especialmente porque podría ser posible hacerlo de forma anónima o, al menos, sin necesidad de mostrarse e identificarse en una comisaría de policía.

3.4. Conclusión

En el ejemplo no existe ninguna disposición específica que pueda servir de base jurídica. Sin embargo, aunque existiera una base jurídica suficiente, no se cumplirían los requisitos de necesidad y proporcionalidad, lo que supondría una injerencia desproporcionada en los derechos del interesado al respeto de su vida privada y a la protección de sus datos personales en virtud de la Carta.

4 SUPUESTO 4:

4.1. Descripción

La policía implanta una forma de identificar a los sospechosos de cometer un delito grave captados por las cámaras de videovigilancia, mediante una TRF retrospectiva. Un agente selecciona manualmente la imagen o imágenes de los sospechosos en el material de vídeo que se ha recogido en el lugar del delito o en otro lugar dentro de una investigación preliminar y, a continuación, envía la imagen o imágenes al departamento forense. Este utiliza la TRF para cotejar las imágenes con fotografías de individuos que la policía ha reunido previamente en una base de datos (la denominada base de datos descriptiva, formada por sospechosos y antiguos condenados). La base de datos descriptiva es analizada para este procedimiento (temporalmente y en un entorno aislado) por medio de la TRF, para poder llevar a cabo el proceso de cotejo. Para minimizar la interferencia con los derechos e intereses de las personas cotejadas, un número muy limitado de empleados del departamento forense tiene permiso para llevar a cabo el cotejo propiamente dicho; el acceso a los datos está restringido a los funcionarios encargados del expediente concreto, y se lleva a cabo un control manual de los resultados antes de transmitir cualquier resultado al funcionario encargado de la investigación. Los datos biométricos no se envían fuera del entorno controlado y aislado. En la investigación posterior solo se utiliza el resultado y la imagen (no la plantilla biométrica). Los

empleados reciben formación específica sobre las normas y procedimientos para este tratamiento, y todo el tratamiento de datos personales y biométricos está suficientemente especificado en la legislación nacional.

Fuente de información:

- Tipos de interesados: ☒ sospechosos identificados a partir de las grabaciones de CCTV
- Origen de la imagen:☒ espacios de acceso público ☒ Internet
- Conexión con la delincuencia: ☒ Temporal directa
  ☒ Geográfica directa
- Modo de captura de la información: ☒ a distancia
- Contexto - afectación de otros derechos fundamentales: Sí, a saber: ☒ Libertad de reunión ☒ Libertad de expresión ☒ varios: __

Base de datos de referencia (con la que se compara la información capturada):

- Especificidad: ☒ bases de datos específicas relacionadas con el ámbito de la delincuencia

Algoritmo:

- Tipo de tratamiento: ☒ Identificación de uno entre muchos

Resultado:

- Impacto: ☒ Directo (por ejemplo, el interesado es detenido o interrogado)
- Decisión automatizada: ☒ NO

Análisis jurídico:

- Marco jurídico aplicable: ☒ Legislación nacional específica sobre este tratamiento (reconocimiento facial) para esa autoridad competente

4.2. Marco jurídico aplicable

En este escenario, la legislación nacional dispone que los datos biométricos pueden utilizarse en la realización de análisis forenses cuando sea estrictamente necesario para identificar a los sospechosos de haber cometido un delito grave, mediante el cotejo de las imágenes de la base de datos descriptiva. La legislación nacional especifica qué datos pueden tratarse, así como los procedimientos para preservar la integridad y la confidencialidad de los datos personales y los procedimientos para su destrucción, proporcionando así garantías suficientes contra el riesgo de abuso y arbitrariedad.

4.3. Necesidad y proporcionalidad

El uso del reconocimiento facial es claramente más eficiente en el tiempo que el cotejo manual en el ámbito forense. La selección manual previa de las imágenes limita las interferencias en comparación con el cotejo de todo el material de vídeo con una base de datos y, de este modo, diferencia y se dirige únicamente a las personas comprendidas por el objetivo de combatir la delincuencia grave. Sin embargo, sigue siendo importante considerar si el cotejo puede realizarse manualmente en un plazo razonable, dependiendo del caso de que se trate. La restricción de las personas con acceso a la tecnología y a los datos personales reduce el impacto en los derechos a la intimidad y a la protección de datos, y además las plantillas biométricas no se almacenan ni se utilizan posteriormente en la investigación. El control manual del resultado implica también una reducción del riesgo de falsos positivos.

4.4. Conclusión

Es importante que la legislación nacional proporcione una base jurídica adecuada para el tratamiento de los datos biométricos, así como para la base de datos nacional con la que se realiza el cotejo. En este escenario se han establecido varias medidas para limitar la interferencia con los derechos de protección de datos, como las condiciones de uso de la TRF especificadas en la base jurídica, el número de personas con acceso a la tecnología y a los datos biométricos, los controles manuales, etc. La TRF mejora significativamente la eficiencia en el trabajo de investigación del departamento forense de la policía, se basa en una legislación que permite a la policía procesar datos biométricos cuando sea absolutamente necesario y, por lo tanto, dentro de estos perímetros puede considerarse una interferencia legal de los derechos del individuo.

5 ESCENARIO 5

5.1. Descripción

La identificación biométrica remota es cuando las identidades de las personas se establecen con la ayuda de identificadores biométricos (imagen facial, forma de andar, iris, etc.) a distancia, en un espacio público y de manera reiterada o continua, cotejándolos con datos (biométricos) almacenados en una base de datos[89]. La identificación biométrica remota se lleva a cabo en tiempo real, si la captura del material de imagen, la comparación y la identificación se producen sin una demora significativa.

Antes de implantar una identificación biométrica remota en tiempo real, la policía elabora una lista de vigilancia de sujetos de interés en el marco de una investigación. La lista incluye imágenes faciales de los individuos. Basándose en el conocimiento de que los individuos pueden hallarse en una zona específica, como un centro comercial o una plaza pública, la policía decide cuándo, dónde y durante cuánto tiempo desplegar la identificación biométrica a distancia.

El día de la actuación, colocan una furgoneta de policía sobre el terreno como centro de control, con un oficial superior de policía a bordo. La furgoneta contiene monitores que muestran imágenes de cámaras de CCTV situadas cerca, ya sea instaladas *ad hoc* o conectando con las señales de las cámaras ya instaladas. A medida que los peatones pasan por las cámaras, la tecnología aísla las imágenes faciales, las convierte en una plantilla biométrica y las compara con las plantillas biométricas de las personas que figuran en la lista de observación.

Si se detecta una posible coincidencia entre la lista de observación y los viandantes, se envía una alerta a los agentes de la furgoneta, que a continuación advierten a los agentes sobre el terreno si la alerta es positiva, por ejemplo, a través de un dispositivo de radio. A continuación, los agentes sobre el terreno deciden si intervienen, se aproximan o, en última instancia, detienen a la persona. Se registran las medidas adoptadas por el funcionario sobre el terreno. En el caso de un control discreto, se almacena la información recogida (por ejemplo, con quién está la persona, cómo va vestida y a dónde se dirige).

La legislación nacional a la que se hace referencia establece una disposición genérica, según la cual el tratamiento de datos biométricos con el fin de identificar de manera unívoca a una persona física es lícito si es estrictamente necesario y está sujeto a garantías adecuadas para los derechos y libertades de la persona interesada.

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Fuente de información:

- Tipos de interesados: ☒ todas las personas
- Origen de la imagen: ☒ espacios de acceso público
- Conexión con la delincuencia:☒ Sin necesidad de una conexión geográfica o temporal directa
- Modo de captura de la información: ☒ a distancia
- Contexto: afecta a otros derechos fundamentales: Sí, a saber: ☒ Libertad de reunión ☒ Libertad de expresión ☒ varios
- Fuentes adicionales de información disponibles sobre el interesado: ☒ otros: no excluidos (por ejemplo, uso de cajeros automáticos o comercios visitados)

Base de datos de referencia (con la que se compara la información capturada):

- Especificidad: ☒ bases de datos específicas relacionadas con el ámbito de la delincuencia

Algoritmo:

- Tipo de tratamiento: ☒ Identificación de uno entre muchos

Resultado:

- Impacto: ☒ Directo (por ejemplo, el interesado puede ser detenido o interrogado)
- Decisión automatizada: ☒ NO
- Duración del almacenamiento: hasta que finalicen todas las investigaciones posibles

Análisis jurídico:

- Tipo de información previa al interesado: ☒ Con carácter general, en el sitio web de la FCS
- Marco jurídico aplicable: ☒ la DAP, esencialmente trasladada a la legislación nacional☒ Ley nacional genérica sobre el uso de datos biométricos por parte de las FCS

5.2. Marco jurídico aplicable

Las bases jurídicas que se limitan a repetir la cláusula general del artículo 10 de la DAP no son lo suficientemente claras en sus términos como para proporcionar a las personas una indicación adecuada de las condiciones y circunstancias en las que las FCS están facultadas para utilizar grabaciones de CCTV de espacios públicos para crear una plantilla biométrica de su cara y compararla con bases de datos policiales. Por lo tanto, el marco jurídico establecido en este escenario no cumple los requisitos mínimos para servir de base jurídica.[90]

5.3. Necesidad y proporcionalidad

El listón de la necesidad y la proporcionalidad se sitúa más alto cuanto mayor es la injerencia. La identificación biométrica remota tiene varias repercusiones en los derechos fundamentales en los espacios públicos:

Los escenarios implican el seguimiento de todos los transeúntes en el espacio público correspondiente. Por lo tanto, afecta gravemente a las razonables expectativas de anonimato de las personas en los espacios públicos[91], que es un requisito necesario para múltiples aspectos del proceso democrático, como la decisión de unirse a una asociación cívica, asistir a reuniones y conocer a personas de cualquier

[90]En los casos en que un proyecto científico destinado a investigar el uso de la TRF necesite tratar datos personales, sin entrar dicho tratamiento en el ámbito de aplicación del artículo 4, apartado 3, de la DAP ni en el ámbito de aplicación del Derecho de la Unión, será aplicable el RGPD. En el caso de proyectos piloto que hayan de preceder a operaciones policiales, seguirá siendo aplicable la DAP.

[91] Respuesta del CEPD a los diputados del Parlamento Europeo sobre la aplicación de reconocimiento facial desarrollada por Clearview AI, 10 de junio de 2020, Ref.: OUT2020-0052.

origen social y cultural, participar en una protesta política y visitar lugares de cualquier tipo. El concepto de anonimato en los espacios públicos es esencial para reunir e intercambiar información e ideas libremente. Preserva la pluralidad de opiniones, la libertad de reunión pacífica, la libertad de asociación y la protección de las minorías, y apoya los principios de separación de poderes y de controles y contrapesos. Una merma del anonimato en los espacios públicos puede generar graves efectos de amedrentamiento en los ciudadanos, que pueden llegar a abstenerse de determinados comportamientos compatibles con una sociedad libre y abierta. Esto afectaría al interés público, ya que una sociedad democrática requiere la autodeterminación y la participación de sus ciudadanos en el proceso democrático.

Si se aplica una tecnología de este tipo, el simple hecho de caminar por la calle, ir al metro o a la panadería en la zona afectada dará lugar a la recopilación de datos personales, incluidos los biométricos, por parte de las fuerzas del orden y, en el primer escenario, también al cotejo con las bases de datos policiales. Una situación en la que se hiciese lo mismo tomando huellas dactilares sería claramente desproporcionada.

El número de interesados afectados es extremadamente elevado, ya que se ven afectadas todas las personas que caminen por la zona pública correspondiente. Además, los escenarios implicarían un tratamiento masivo automatizado de los datos biométricos, así como un cotejo masivo de los datos biométricos con bases de datos policiales.

En la jurisprudencia europea, la vigilancia masiva está prohibida (por ejemplo, el TEDH, en el asunto S. y Marper contra Reino Unido, consideró la retención indiscriminada de datos biométricos como una «injerencia desproporcionada» en el derecho a la intimidad, ya que no puede considerarse «necesaria en una sociedad democrática»).

La identificación biométrica a distancia es tan propensa a la vigilancia masiva que no existen medios fiables de restricción. Es esencialmente diferente de la videovigilancia como tal, ya que el posible uso de imágenes de vídeo sin identificación biométrica es ya una interferencia fuerte, pero al mismo tiempo limitada, mientras que si se aplica la TRF, el ya amplio sistema de videovigilancia como principal fuente de los datos sufrirá un salto cualitativo. Además, especialmente en lo que respecta a los efectos disuasorios implícitos, no serán visibles las posibles restricciones en la aplicación de las instalaciones de videovigilancia ya existentes, por lo que el público no confiará en ellas.

La identificación biométrica a distancia por parte de las autoridades policiales trata a todo el mundo como un potencial sospechoso. Sin embargo, en un Estado sujeto al Estado de Derecho, se presume que los ciudadanos son inocentes mientras no se demuestre lo contrario. Este principio también se refleja en parte en la DAP, que subraya la necesidad de distinguir, en la medida de lo posible, entre el tratamiento de condenados o sospechosos, para el que la autoridad judicial debe tener *«motivos fundados para presumir que han cometido o van a cometer una infracción penal»* [artículo 6, letra a), de la DAP], y los que no están condenados ni son sospechosos de una actividad delictiva.

Si se aplica en puntos nodales de transporte o en espacios públicos, y las FCS utilizan una tecnología capaz de identificar de manera unívoca a una sola persona, así como de rastrear y analizar su paradero y movimientos, se revelará hasta la información más sensible sobre las personas (preferencias sexuales, religión, problemas de salud), lo que implica un enorme riesgo de acceso y uso ilícitos de los datos.

La instalación de un sistema que permite averiguar los aspectos más íntimos del comportamiento y las características de una persona genera graves efectos disuasorios. Hace que las personas se pregunten si deben acudir a una determinada manifestación, lo cual menoscaba el proceso democrático. También

podría considerarse problemático reunirse y ser visto en público con un cierto amigo conocido por tener problemas con la policía, o comportarse de manera poco convencional, ya que todo ello daría lugar a la atracción del algoritmo del sistema y, por tanto, a medidas policiales.

Es imposible proteger a los interesados vulnerables, como los niños. Además, se ven afectadas las personas que tienen un interés profesional (y a menudo una obligación legal) por mantener sus contactos confidenciales, como los periodistas, los abogados y el clero. Esto podría dar lugar, por ejemplo, a la revelación de la fuente y del periodista, o al hecho de que una persona consulte a un abogado penalista. El problema no solo afecta a los lugares públicos aleatorios, donde se reúnen, por ejemplo, los periodistas y sus fuentes, sino naturalmente también a los espacios públicos necesarios para acercarse y acceder a las instituciones o a los profesionales del sector.

Además, el malestar de las personas con la TRF puede llevarles a cambiar su comportamiento, evitando los lugares en los que está implantada, retirándose así de la vida social y de acontecimientos culturales. Dependiendo del alcance del despliegue de la TRF, el impacto en las personas puede ser tan significativo como para afectar a su capacidad para llevar una vida digna[92].

Por lo tanto, existe una alta probabilidad de afectar a la esencia (el núcleo inviolable) del derecho a la protección de los datos personales. Son indicios sólidos (véase la sección 3.1.3.2 de las directrices), en particular, los siguientes: a gran escala, las autoridades policiales someten a tratamiento automático las características biológicas únicas de las personas con algoritmos basados en la verosimilitud con solo una explicación limitada de los resultados. Las limitaciones a los derechos a la intimidad y a la protección de datos se imponen con independencia del comportamiento individual de la persona o de las circunstancias que le afecten. Desde el punto de vista estadístico, casi todos los interesados afectados por esta injerencia son personas que respetan la ley. Solo existen posibilidades limitadas de facilitar información al interesado. En la mayoría de los casos, el amparo judicial solo será posible posteriormente.

La confianza en un sistema basado en la verosimilitud y con una explicabilidad limitada puede conducir a la difusión de la responsabilidad, y los déficits en la protección pueden ser un incentivo para la negligencia.

Una vez que se utiliza un sistema de este tipo, que puede aplicarse también a las cámaras de videovigilancia existentes, con muy poco esfuerzo y sin que sea visible para las personas, puede utilizarse indebidamente y permitir la elaboración sistemática y rápida de listas de personas según su origen étnico, sexo, religión, etc. El principio del tratamiento de datos personales con arreglo a criterios predeterminados, como el paradero de una persona y el itinerario recorrido, ya se practica[93] y es propenso a la discriminación.

Habida cuenta de la sensibilidad, la expresividad y la cantidad de datos tratados, los sistemas de reconocimiento facial a distancia en lugares de acceso público tienden a ser utilizados indebidamente, con efectos perjudiciales para las personas afectadas. Estos datos también pueden recopilarse con

[92] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, página 20.

[93] Véase el artículo 6 de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de miércoles, 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, y el artículo 33 del Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de miércoles, 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226.

facilidad y utilizarse indebidamente para presionar a actores clave siguiendo el principio de controles y contrapesos, como la oposición política, los funcionarios y los periodistas.

Por último, los sistemas de TRF tienden a presentar fuertes efectos de sesgo en relación con la raza y el género: los falsos positivos afectan de manera desproporcionada a las personas de color y a las mujeres[94], lo que da lugar a discriminación. Las medidas policiales adoptadas a raíz de un falso positivo, como registros y detenciones, estigmatizan aún más a estos grupos.

5.4. Conclusión

Los supuestos mencionados anteriormente relativos al tratamiento a distancia de datos biométricos en espacios públicos con fines de identificación no logran un equilibrio justo entre los intereses públicos y privados concurrentes, lo que constituye una injerencia desproporcionada en los derechos del interesado en virtud de los artículos 7 y 8 de la Carta.

6 ESCENARIO 6

6.1. Descripción

Una entidad privada proporciona una aplicación en la que se extraen imágenes faciales de Internet para crear una base de datos. El usuario (por ejemplo, la policía) puede entonces cargar una imagen y, mediante la identificación biométrica, la aplicación intentará cotejarla con las imágenes faciales o las plantillas biométricas en su base de datos.

Un departamento de policía local está llevando a cabo una investigación de un delito registrado en vídeo en el que no se puede identificar a varios testigos y sospechosos potenciales mediante el cotejo de la información recopilada con las bases de datos o la inteligencia interna. Según la información recogida, las personas no están registradas en ninguna base de datos policial existente. La policía decide utilizar una herramienta como la descrita anteriormente, proporcionada por una empresa privada, para identificar a las personas mediante la identificación biométrica.

Fuente de información:

- Tipos de interesados: ☒ todos los ciudadanos (testigos) ☒ condenados ☒ sospechosos
- Origen de la imagen: ☒ Imágenes de vídeo de un lugar público o recogidas en otro lugar en el marco de una investigación preliminar
- Conexión con la delincuencia: ☒ No es necesaria
- Modo de captura de la información: ☒ a distancia
- Contexto: afecta a otros derechos fundamentales: Sí, a saber: ☒ Libertad de reunión ☒ Libertad de expresión ☒ varios: __

Base de datos de referencia (con la que se compara la información capturada):

- Especificidad: ☒ bases de datos de uso general extraídas de Internet

Algoritmo:

- Tipo de tratamiento: ☒ identificación de uno entre muchos

Resultado:

- Impacto ☒ Directo (por ejemplo, el interesado es detenido, interrogado, comportamiento discriminatorio)

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

- Decisión automatizada: ☒ NO

Análisis jurídico:

- Tipo de información previa al interesado: ☒ No

6.2. Marco jurídico aplicable

Cuando una entidad privada presta un servicio que incluye un tratamiento de datos personales para el que determina la finalidad y los medios (en este caso, el «arrastre» de imágenes de internet para crear una base de datos), dicha entidad privada debe tener una base jurídica para este tratamiento. Además, la autoridad policial que decida utilizar este servicio para sus fines debe contar con una base jurídica para el tratamiento cuyos fines y los medios ella misma determine. Para que la autoridad policial pueda tratar datos biométricos debe existir un marco jurídico que especifique el objetivo, los datos personales que se tratarán, los fines del tratamiento y los procedimientos para preservar la integridad y la confidencialidad de los datos personales, así como los procedimientos para su destrucción.

Este escenario implica la recogida masiva de datos personales de individuos que no son conscientes de que sus datos están siendo recogidos. Dicho tratamiento solo puede ser lícito en circunstancias muy excepcionales. Dependiendo de dónde se encuentre la base de datos, el uso de un servicio de este tipo puede implicar la transferencia de datos personales y/o categorías especiales de datos personales fuera de la Unión Europea (por parte de la policía, por ejemplo, «enviando» la imagen facial en el vídeo de vigilancia o recopilada de otro modo), lo que requiere condiciones específicas para dicha transferencia (véase el artículo 39 de la DAP).

No existen normas específicas en este escenario que permitan este tratamiento por parte de la autoridad policial.

6.3. Necesidad y proporcionalidad

El uso del servicio por parte de las autoridades policiales significa que los datos personales se comparten con una entidad privada que utiliza una base de datos en la que los datos personales se recogen de forma ilimitada y a gran escala. No existe ninguna conexión entre los datos personales recogidos y el objetivo perseguido por la autoridad policial. El intercambio de datos entre esta y la entidad privada también implica una falta de control por parte de la autoridad sobre los datos tratados por la entidad privada y una gran dificultad para que los interesados ejerzan sus derechos, ya que no serán conscientes de que sus datos se tratan de este modo. Esto lleva a que se sitúe muy elevado el listón de las situaciones en las que dicho tratamiento pueda siquiera llevarse a cabo. Es cuestionable si cualquier objetivo cumpliría los requisitos establecidos en la Directiva, ya que las excepciones y limitaciones a los derechos a la intimidad y a la protección de datos solo son lícitas cuando resultan estrictamente necesarias. El interés general de eficacia en la lucha contra los delitos graves no justifica por sí solo el tratamiento cuando se recogen indiscriminadamente cantidades tan grandes de datos. Por lo tanto, este tratamiento no cumpliría los requisitos de necesidad y proporcionalidad.

6.4. Conclusión

La falta de normas claras, precisas y previsibles que cumplan los requisitos de los artículos 4 y 10 de la Directiva, así como la falta de pruebas de que este tratamiento es estrictamente necesario para alcanzar los objetivos perseguidos, lleva a la conclusión de que el uso de esta aplicación no cumple los requisitos de necesidad y proporcionalidad y constituye una interferencia desproporcionada en los derechos de los interesados al respeto de la vida privada y la protección de los datos personales en virtud de la Carta.