GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

00727/12/ES
WP 192

Dictamen 02/2012 sobre reconocimiento facial en los servicios en línea y móviles

adoptado el 22 de marzo de 2012

1. Introducción

En los últimos años, la disponibilidad y la precisión de la tecnología de reconocimiento facial han avanzado rápidamente. Por añadidura, esta tecnología ha sido integrada en los servicios en línea y móviles para la identificación, la autenticación/verificación o la categorización de las personas. Esta tecnología que antes parecía propia de la ciencia ficción, ahora está a disposición tanto de las organizaciones públicas como de las privadas. Entre los servicios en línea y móviles que la utilizan se encuentran las redes sociales y los fabricantes de teléfonos «inteligentes».

El Grupo de Trabajo del Artículo 29 (WP29), en su Documento de trabajo sobre biometría (WP80) y en su Dictamen 03/2012 (WP193) sobre avances en las tecnologías biométricas, publicado recientemente, ya había considerado la capacidad de capturar datos automáticamente y reconocer una cara a partir de una imagen digital. Se considera que el reconocimiento facial está incluido en el ámbito de la biometría ya que en muchos casos contiene los detalles suficientes para identificar a una persona de manera inequívoca.

El Dictamen 03/2012 observa que:

> *[la biometría] permite el seguimiento, localización o establecimiento del perfil automatizados de las personas y, como tal, sus efectos potenciales sobre la intimidad y el derecho a la protección de los datos personales son importantes.*

Esta afirmación es especialmente cierta en lo que respecta al reconocimiento facial en los servicios en línea y móviles que pueden captar imágenes de una persona (con o sin su conocimiento) y transmitirlas a continuación a un servidor remoto para su tratamiento. Los servicios en línea, muchos de los cuales pertenecen a entidades privadas que se encargan de explotarlos, han acumulado vastos archivos de imágenes cargadas por los propios individuos. En algunos casos, esas imágenes pueden haber sido obtenidas ilícitamente, recuperándolas de otros sitios públicos como las memorias caché de los motores de búsqueda. Los pequeños dispositivos móviles que cuentan con cámaras de alta resolución permiten a sus usuarios obtener imágenes y conectarse en tiempo real a servicios en línea a través de conexiones permanentes. En consecuencia, los usuarios pueden compartir esas imágenes con otras personas o llevar a cabo una identificación, autenticación/verificación o categorización para acceder a información adicional sobre la persona, conocida o desconocida, que se encuentra delante de ellos.

Por tanto, el reconocimiento facial en los servicios en línea y móviles merece una atención especial por parte del Grupo de Trabajo del Artículo 29, ya que el uso de esta tecnología suscita muchas preocupaciones en lo que respecta a la protección de los datos.

El objetivo del presente Dictamen es analizar el marco jurídico y presentar recomendaciones adecuadas aplicables a las tecnologías de reconocimiento facial cuando se utilizan en el contexto de servicios en línea y móviles. Este Dictamen se dirige a las autoridades legislativas europeas y nacionales, los responsables del tratamiento de datos y los usuarios de tales tecnologías. No pretende repetir los principios a que hacía referencia en el Dictamen 03/2012, sino que más bien se inspira en ellos en el contexto de los servicios en línea y móviles.

2. Definiciones

La tecnología de reconocimiento facial no es algo nuevo, y existen ya muchas definiciones e interpretaciones de su terminología. Por ello conviene definirla claramente en el contexto del presente Dictamen.

Imagen digital: Una imagen digital es una representación bidimensional de una imagen en forma digital. No obstante, los últimos avances en tecnología de reconocimiento facial requieren la inclusión de imágenes tridimensionales, además de las imágenes estáticas y en movimiento (es decir, fotografías y videos grabados y en directo).

Reconocimiento facial: El reconocimiento facial es el tratamiento automático de imágenes digitales que contienen las caras de personas a fines de identificación, autenticación/verificación o categorización[1] de dichas personas. El proceso de reconocimiento facial está compuesto por una serie de subprocesos diferenciados:

a) Obtención de la imagen: Es el proceso de captar la cara de una persona y convertirla en formato digital (la imagen digital). En un servicio en línea y móvil, la imagen puede haberse obtenido en un sistema diferente, por ejemplo, haciendo una fotografía con una cámara digital que, a continuación, se transfiere a un servicio en línea.

b) Detección de la cara: En este proceso se detecta la presencia de una cara dentro una imagen digital y se marca la zona.

c) Normalización: Es el proceso de atenuar las variantes entre las regiones faciales detectadas, por ejemplo, convirtiéndolas en dimensiones estándar, rotándolas o alineando las distribuciones de los colores.

d) Extracción de características: Es el proceso de aislar y extraer las características reproductibles y distintivas de la imagen digital de una persona. La extracción de características puede ser holística[2], basada en las características[3] o una combinación de ambos métodos[4]. El conjunto de características clave puede almacenarse en una plantilla[5] para ser comparado posteriormente.

e) Registro: Cuando una persona se somete por primera vez a un determinado sistema de reconocimiento facial, la imagen y/o la plantilla pueden almacenarse como registro para comparaciones posteriores.

f) Comparación: Es el proceso de medir la similitud existente entre un conjunto de características (la muestra) y otro registrado previamente en el sistema. Los principales objetivos de la comparación son la identificación y la autenticación/verificación. Un tercer objetivo de la comparación es la categorización, que consiste en extraer las características de una imagen de una persona a fin de

1 Identificación, autenticación/verificación y categorización se definen en el documento 03/2012.

2 Extracción holística de características: representación matemática de una imagen completa como la resultante de un análisis de los componentes principales.

3 Extracción basada en las características: identificación de la ubicación de características faciales específicas, como los ojos, la nariz y la boca.

4 Conocido también como método híbrido de extracción de características.

5 La plantilla se define en el Dictamen 03/2012 como las características esenciales extraídas de los datos biométricos en forma bruta (por ej., las mediciones faciales de una imagen) y almacenadas para su tratamiento posterior, más que los datos brutos en sí mismos.

clasificarla en una o varias categorías generales (edad, sexo, color de la ropa, etc.). Un sistema de categorización no tiene por qué tener un proceso de registro.

3. Ejemplos de reconocimiento facial en servicios en línea y móviles

El reconocimiento facial puede estar incorporado a servicios en línea y móviles de diversas maneras y para distintos fines. En el presente Dictamen, el Grupo de Trabajo del Artículo 29 se centra en una serie de ejemplos diferentes que tienen como objetivo ofrecer un contexto adicional para el análisis jurídico e incluyen la utilización del reconocimiento facial a fines de identificación, autenticación/verificación y categorización.

3.1. El reconocimiento facial como medio de identificación

Ejemplo 1: Los servicios de redes sociales (*social networking services* (SNS)[6] permiten a los usuarios adjuntar una imagen digital a sus perfiles. Además, los usuarios pueden poner imágenes en línea para compartirlas con otros usuarios, registrados o no. Los usuarios registrados pueden identificar y etiquetar manualmente a otras personas (que pueden o no ser usuarios registrados) en las imágenes que publican en línea. Dichas etiquetas pueden ser visionadas por su creador, compartidas con un grupo más amplio de amigos o compartidas con todos los usuarios registrados o no. El servicio de red social puede utilizar las imágenes etiquetadas a fin de crear una plantilla para cada usuario registrado y, utilizando un sistema de reconocimiento facial, sugerir automáticamente etiquetas para las nuevas fotografías que se vayan publicando en línea.

Un motor de búsqueda de Internet podría acceder posteriormente a estas imágenes de personas publicadas por los usuarios y almacenarlas en una memoria caché. El motor de búsqueda podría decidir desarrollar más sus funciones de búsqueda permitiendo que los usuarios carguen una imagen de una persona y ofreciéndoles los resultados que presenten la mayor coincidencia, junto con un vínculo a la página de perfil de la red social. La imagen cargada puede ser obtenida directamente desde la cámara de un «teléfono inteligente».

3.2. El reconocimiento facial como medio de autenticación/verificación

Ejemplo 2: Es cuando en lugar de un nombre de usuario y contraseña se utiliza un sistema de reconocimiento facial para controlar el acceso a un servicio o a un dispositivo en línea o móvil. Para efectuar el registro se utiliza una cámara incorporada al dispositivo que obtiene una fotografía del usuario autorizado y se crea una plantilla que puede almacenarse en el dispositivo o en un servidor remoto en el servicio en línea. Cada vez que la persona desea acceder al servicio o al dispositivo, se obtiene una nueva fotografía suya que se compara con la imagen de referencia. Si el sistema determina que la coincidencia es positiva, se le autoriza el acceso.

[6] Los servicios de redes sociales se definen, de manera general, en el Dictamen 5/2009 sobre las redes sociales en líneas como *«plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes»*.

3.3. El reconocimiento facial como medio de categorización

Ejemplo 3: El servicio de red social descrito en el ejemplo 1 puede autorizar el acceso a su archivo de imágenes a una tercera empresa que explote un servicio de reconocimiento facial en línea. El servicio autoriza a los clientes de esa tercera empresa a incorporar tecnología de reconocimiento facial en otros productos. Esta funcionalidad permite a esos otros productos presentar imágenes de personas a fin de detectar y clasificar las caras en un conjunto de criterios predefinidos, como edad, sexo y preferencias.

Ejemplo 4: Una consola de videojuegos está provista de un sistema de control mediante gestos que detecta los movimientos del usuario para controlar el juego. La cámara o cámaras utilizadas para el sistema de control mediante gestos comparte las fotografías de las personas con un sistema de reconocimiento facial que predice la edad, sexo y preferencias probables de la persona que está jugando. Entonces estos datos, así como los procedentes de otros factores multimodales, pueden alterar la configuración del juego para mejorar la experiencia del usuario o alterar el entorno a fin de adaptarlo al perfil previsto del mismo. De manera similar, un sistema podría clasificar a los usuarios para permitirles o denegarles el acceso a contenidos no aptos para menores, o para mostrar publicidad selectiva dentro del juego.

4. Marco jurídico

El marco jurídico aplicable al reconocimiento facial es el de la Directiva de protección de datos (95/46/CE), que ya se ha analizado a este respecto en el Dictamen 03/2012. Esta sección únicamente pretende presentar un resumen del marco jurídico en el contexto del reconocimiento facial en los servicios en línea y móviles basándose en los ejemplos que figuran en la sección 3. En el Dictamen 03/2012 se presentan más ejemplos de reconocimiento facial.

4.1. Las imágenes digitales como datos personales

Si en una imagen digital se distingue tan claramente el rostro de una persona que es posible identificarla, dicha imagen se consideraría un dato personal. Ello dependerá de una serie de parámetros, como la calidad de la imagen o el encuadre concreto. En la mayoría de los casos no se considerarían datos personales las imágenes de escenas en las que se ve a personas en la distancia, o en las que los rostros están difuminados. No obstante, es importante observar que las imágenes digitales pueden incluir datos personales de más de una persona (por ej., en el ejemplo 4 pueden aparecer varios jugadores en el marco de captación de la cámara), y el hecho de que aparezcan otras personas en la fotografía podría implicar la existencia de una relación.

El Dictamen 04/2007 sobre el concepto de datos personales reitera el punto de que si un dato se refiere a una persona o si «*hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa*», se considera un dato personal.

Por definición, una plantilla creada a partir de una imagen de una persona también es un dato personal desde el momento en que contiene un conjunto de características distintivas de su rostro que se asocian a una persona concreta y se almacenan como referencia para comparaciones futuras en procesos de identificación y autenticación/verificación.

Una plantilla o conjunto de características distintivas utilizada únicamente en un sistema de categorización no contiene, en general, información suficiente para identificar a una persona. Solamente debería incluir la información suficiente para llevar a cabo la categorización (por ej., hombre o mujer). En tal caso, no sería un dato personal, siempre que la plantilla (o el

resultado) no vaya asociada al registro, el perfil o la imagen original de la persona (que sí se consideran datos personales).

Además, puesto que tanto las imágenes digitales de las personas como las plantillas se refieren a las «*propiedades biológicas, aspectos de comportamiento, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables*»[7], deben considerarse datos biométricos.

4.2. Las imágenes digitales como categoría especial de datos personales

En determinados casos las imágenes digitales de personas pueden considerarse una categoría especial de datos personales[8]. Concretamente, cuando las plantillas o las imágenes digitales de personas son tratadas posteriormente para obtener categorías especiales de datos, se considerarán incluidas en esta categoría especial. Así sucede, por ejemplo, si van a utilizarse para obtener información sobre el origen étnico, la religión o la salud de las personas afectadas.

4.3. Tratamiento de datos personales en el contexto de un sistema de reconocimiento facial

Como ya se ha explicado, el reconocimiento facial se basa en una serie de etapas de tratamiento automatizado. En consecuencia, el reconocimiento facial constituye una forma automatizada de tratamiento de datos personales que incluye datos biométricos.

Por el hecho de utilizar datos biométricos, los sistemas de reconocimiento facial pueden estar sometidos a controles adicionales o a otras disposiciones legislativas en los distintos Estados miembros, como la autorización previa o la legislación laboral. En el Dictamen 03/2012 se analiza más detenidamente el recurso a la biometría en el contexto laboral.

4.4. Responsable del tratamiento de los datos

Volviendo a los ejemplos anteriores, los responsables del tratamiento de los datos serán, generalmente, los propietarios del sitio web y/o los proveedores de servicios en línea, así como los operadores de aplicaciones móviles que utilicen el reconocimiento facial, puesto que determinan los objetivos y los medios del tratamiento[9]. Ello incluye la conclusión formulada en el Dictamen 05/2009 sobre las redes sociales en línea en el sentido de que *«Los proveedores de SRS son responsables del tratamiento de datos en virtud de la Directiva relativa a la protección de datos»*.

4.5. Motivo legítimo

La Directiva 95/46/CE establece las condiciones que debe cumplir el tratamiento de los datos personales. Ello implica que, en primer lugar, el tratamiento debe cumplir los requisitos relativos a la calidad de los datos (artículo 6). En el caso que nos ocupa las imágenes digitales de las personas y las plantillas correspondientes deberán ser «pertinentes» y «no excesivas» a fines del tratamiento para el reconocimiento facial. Por otra parte, el tratamiento solo podrá efectuarse si se cumple uno de los criterios especificados en el artículo 7.

Debido a los riesgos particulares asociados a los datos biométricos, antes de comenzar el tratamiento de las imágenes digitales a fines del reconocimiento facial se requerirá el consentimiento informado de la persona. No obstante, en algunos casos es posible que el responsable del tratamiento de los datos necesite llevar a cabo algunas etapas del proceso de

---

7 Definición de datos biométricos en el Dictamen 03/2012.

8 La jurisprudencia de determinados países clasifica las imágenes digitales de caras como una categoría de datos especial - LJN BK6331 Tribunal Superior de los Países Bajos, 23 de marzo de 2010.

9 Dictamen 01/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»

reconocimiento facial con el objetivo, precisamente, de comprobar si el usuario ha dado o no su consentimiento, que es la base legal del tratamiento. En tal caso el tratamiento inicial (es decir, la obtención de la imagen, la detección de la cara, la comparación, etc.) puede tener una base legal distinta, especialmente el interés legítimo del responsable del tratamiento de los datos en cumplir las normas sobre protección de datos. Los datos procesados durante estas fases solo deberán utilizarse con el objetivo estrictamente limitado de comprobar el consentimiento del usuario, y deberán eliminarse inmediatamente después.

En el Ejemplo 1, el responsable del tratamiento de los datos ha determinado que todas las nuevas imágenes publicadas en línea por usuarios registrados de las redes sociales serán sometidas a detección de la cara, extracción de características y comparación. Solo se producirán coincidencias con estas nuevas imágenes en aquellos usuarios registrados para los que exista una plantilla inscrita en la base de datos de identificación, a los que, por tanto, se les sugerirá una etiqueta de manera automática. Si se considerara que el consentimiento de la persona es la única base legítima para la totalidad del tratamiento de los datos, el servicio completo se bloquearía ya que, por ejemplo, no hay forma de obtener el consentimiento de los usuarios no registrados cuyos datos personales pueden ser objeto de tratamiento durante la detección de la cara y la extracción de características. Además, no sería posible distinguir entre las caras de los usuarios registrados que hayan otorgado su consentimiento o no lo hayan hecho sin efectuar antes el reconocimiento facial. Solo tras la identificación (o la no identificación), el responsable del tratamiento de los datos podrá determinar si cuenta o no con el consentimiento adecuado para ese tratamiento específico.

Antes de que un usuario registrado publique una imagen en una red social deberá haber sido informado claramente de que esas imágenes serán sometidas a un sistema de reconocimiento facial. Lo que es más importante, también deberá haberse ofrecido a los usuarios registrados la opción de autorizar o no que sus plantillas de referencia se incluyan en la base de datos de identificación. Consecuentemente, ni a los usuarios no registrados ni a los usuarios registrados que no hayan autorizado el tratamiento se les sugerirá automáticamente una etiqueta con su nombre, ya que las imágenes en las que aparezcan no coincidirán con plantilla alguna.

El consentimiento otorgado por el usuario que publica una imagen no debería confundirse con la necesidad de contar con una base legítima para el tratamiento de los datos personales de otras personas que pudieran aparecer en la imagen. Con este fin, el responsable del tratamiento de los datos podría basarse en un motivo legítimo diferente para el tratamiento en las fases intermedias (detección de la cara, normalización y comparación), como el de que ello es en su interés legítimo, siempre que se apliquen las restricciones y controles suficientes para proteger las libertades y derechos fundamentales de las personas afectadas que no sean la persona que publica la imagen. Uno de tales controles sería garantizar que, una vez que no se haya obtenido una coincidencia, no se conservará dato alguno resultante del tratamiento (es decir, que todas las plantillas y los datos asociados sean eliminados de forma segura). Asimismo, el responsable del tratamiento de los datos podría considerar facilitar herramientas a sus usuarios para que cuando publiquen una imagen puedan difuminar las caras de las personas que no coinciden con plantilla alguna de la base de datos de referencia. El registro de la plantilla de una persona en una base de datos de identificación (que permitirá la búsqueda de coincidencias y la consiguiente sugerencia de etiquetas) solo será posible con su consentimiento informado.

Evidentemente, en el Ejemplo 2 durante el proceso de registro puede obtenerse el consentimiento de la persona a la que se autoriza el acceso. Para que este consentimiento sea válido debe establecerse un sistema de control de acceso alternativo e igualmente seguro

(como una contraseña segura). Esta opción alternativa para proteger la intimidad debería proponerse por defecto. Cuando una persona se pone frente a una cámara conectada al dispositivo con el objetivo explícito de obtener acceso, puede considerarse que consiente en el tratamiento de sus datos faciales necesario para la autenticación, incluso si esa persona no es un usuario autorizado del dispositivo. No obstante, la información facilitada debe ser suficiente para garantizar que el consentimiento es válido.

La explotación posterior del archivo de fotos del servicio de redes sociales descrito en el ejemplo 3 constituiría un caso claro de violación del principio de limitación de finalidad y, en consecuencia, debe obtenerse el consentimiento válido de la persona antes de introducir esa funcionalidad, indicando claramente que se realizará dicho tratamiento de imágenes. Lo mismo sucede con el motor de búsqueda descrito en el ejemplo 1. Las imágenes obtenidas por el motor de búsqueda se mostraban para ser vistas, y no para ser tratadas por un sistema de reconocimiento facial. Habría que exigir al proveedor del motor de búsqueda que obtenga el consentimiento de las personas afectadas antes de incorporarlas al segundo sistema de reconocimiento facial.

Así sucedería también en el ejemplo 4, ya que el usuario tal vez no espere que las imágenes captadas para el control por gestos sean sometidas a un tratamiento posterior. Si el responsable del tratamiento de los datos pide el consentimiento de los usuarios para el tratamiento de sus datos a más largo plazo (a lo largo del tiempo o de una parte a otra del juego), deberá recordarles periódicamente que el sistema está activado y garantizar que esté desactivado por defecto.

El Dictamen 15/2011 sobre la definición del consentimiento analiza la calidad, accesibilidad y visibilidad de la información referente al tratamiento de los datos personales. El Dictamen afirma:

> *«La información debe comunicarse directamente a las personas. No basta con que la información esté «disponible» en algún lugar.»*

En consecuencia, la información relativa a la función de reconocimiento facial de un servicio móvil o en línea no debe estar oculta, sino que debe estar disponible de forma fácilmente accesible y comprensible. Ello incluirá garantizar que las propias cámaras no estén funcionando de manera disimulada. Los responsables del tratamiento de los datos deben tener en cuenta las expectativas razonables de privacidad de los usuarios cuando apliquen tecnologías de reconocimiento facial, y tratar estos temas de manera adecuada.

En este contexto, el consentimiento otorgado para la inscripción no puede derivarse de la aceptación por parte del usuario de los términos y condiciones generales del servicio subyacente, a no ser que el objetivo fundamental del servicio implique presumiblemente el reconocimiento facial. Ello se debe al hecho de que, en la mayoría de los casos, la inscripción es una funcionalidad suplementaria y no está directamente relacionada con el funcionamiento del servicio móvil o en línea. Los usuarios no tienen por qué esperar necesariamente que esa funcionalidad esté activada cuando utilizan el servicio. A este fin, deberá facilitarse explícitamente a los usuarios la posibilidad de otorgar su consentimiento para esta funcionalidad, bien durante el proceso de registro o bien posteriormente, dependiendo de cuando se introduzca la funcionalidad.

Para que el consentimiento se considere válido deberá haberse facilitado la información adecuada sobre el tratamiento de los datos. Siempre deberá ofrecerse a los usuarios la

posibilidad de retirar su consentimiento de manera sencilla. Si se retira el consentimiento, el tratamiento a fines de reconocimiento facial deberá interrumpirse inmediatamente.

5. Riesgos particulares y recomendaciones

Los riesgos para la intimidad de las personas que pueda plantear un sistema de reconocimiento facial dependerán totalmente del tipo de tratamiento y de los objetivos de que se trate. No obstante, existen algunos riesgos que tienen mayor relevancia en fases concretas del reconocimiento facial. En la siguiente sección se ponen de manifiesto los principales riesgos y se formulan recomendaciones de buenas prácticas.

5.1. Tratamiento ilícito a fines de reconocimiento facial

En un entorno en línea, el responsable del tratamiento de los datos puede obtener las imágenes de muchas maneras, por ejemplo, facilitadas por los usuarios del servicio en línea o móvil, sus amigos y colegas o un tercero. En las imágenes pueden figurar las caras de los propios usuarios o de otros usuarios registrados o no registrados, o pueden haber sido obtenidas sin el conocimiento de la persona afectada. Independientemente de los medios por los que las imágenes hayan sido obtenidas, es necesaria una base jurídica para su tratamiento.

Recomendación 1: Si el responsable del tratamiento de los datos está obteniendo la imagen directamente (como en los ejemplos 2 y 4), debe asegurarse de tiene el consentimiento válido de las personas afectadas antes de la obtención y facilitar suficiente información sobre cuando está funcionando una cámara con fines de reconocimiento facial.

Recomendación 2: Si los usuarios están obteniendo imágenes digitales y publicándolas en servicios en línea y móviles con fines de reconocimiento facial, el responsable del tratamiento de los datos debe asegurarse de que las personas que han publicado las imágenes han otorgado su consentimiento para el tratamiento de las mismas que puede tener lugar a fines de reconocimiento facial.

Recomendación 3: Si el responsable del tratamiento de los datos está obteniendo imágenes digitales de personas facilitadas por terceras personas (por ej., copiadas de un sitio web o compradas a un responsable del tratamiento diferente), deberá analizar cuidadosamente la fuente y el contexto en el que se han obtenido y procesado las imágenes únicamente si las personas afectadas han otorgado su consentimiento para tal tratamiento.

Recomendación 4: Los responsables del tratamiento de los datos deben asegurarse de que las imágenes digitales y las plantillas únicamente se utilizan para el objetivo especificado para el que han sido facilitadas. Deberían establecer controles técnicos para reducir el riesgo de que las imágenes digitales sean sometidas a tratamientos posteriores por parte de terceros para fines a los que el usuario no ha dado su consentimiento. Deberían incorporar herramientas para que los usuarios controlen la visibilidad de las imágenes que hayan publicado cuando la configuración por defecto sea restringir el acceso por parte de terceros.

Recomendación 5: Los responsables del tratamiento de los datos deberán asegurarse de que las imágenes digitales de las personas que no sean usuarios registrados del servicio o no hayan dado su consentimiento en otra forma para tal tratamiento únicamente sean objeto de tratamiento en la medida en que el responsable de los datos tenga un interés legítimo en el mismo. Por ejemplo, en el caso del ejemplo 1, para interrumpir el tratamiento y eliminar todos los datos cuando no se de una coincidencia.

Violación de la seguridad durante el tránsito

En el caso de los servicios en línea y móviles es probable que los datos sean transferidos desde el momento de obtención de la imagen hasta las demás fases del tratamiento (por ej., cuando se transfiere una imagen desde una cámara a un sitio web para la extracción de características y la comparación).

Recomendación 6: El responsable del tratamiento de los datos deberá tomar las medidas necesarias para garantizar la seguridad en la transferencia de los datos. Ello puede incluir canales de comunicación codificados o la codificación de la propia imagen. Siempre que sea posible, y especialmente cuando se trate de una autenticación/verificación, se deberá optar por el tratamiento local de los datos.

5.2. Detección facial, normalización y extracción de características

Minimización de los datos

Las plantillas generadas por un sistema de reconocimiento facial pueden contener más datos de los necesarios para el fin o los fines previstos.

Recomendación 7: Los responsables del tratamiento de los datos deberán garantizar que los datos extraídos de una imagen digital para elaborar una plantilla no sean excesivos y contengan solamente la información necesaria para el fin previsto, evitando así cualquier tratamiento posible en el futuro. Las plantillas no deberían ser transferibles de un sistema de reconocimiento facial a otro.

Violación de la seguridad durante el almacenamiento de los datos

Es probable que la identificación y la autenticación/verificación requieran el almacenamiento de la plantilla para utilizarla en comparaciones posteriores.

Recomendación 8: El responsable del tratamiento de los datos deberá analizar cuál es la ubicación más adecuada para su almacenamiento. Ello puede ser en el dispositivo del usuario o en el interior de los sistemas del responsable del tratamiento. El responsable del tratamiento de los datos deberá tomar las medidas necesarias para garantizar la seguridad de los datos almacenados, como codificar la plantilla. No se deberá poder acceder sin autorización a la plantilla o a la ubicación en que estén almacenados los datos. Especialmente cuando se trate de reconocimiento facial a fines de verificación, podrán utilizarse técnicas biométricas de cifrado; en estas técnicas la clave de cifrado está vinculada directamente a los datos biométricos y solo puede recrearse cuando en el momento de la verificación se presenta la muestra biométrica correcta en directo, sin que se haya almacenado imagen o plantilla alguna (constituyendo así un tipo de «biometría indetectable»).

Acceso de las personas afectadas

Recomendación 9: El responsable del tratamiento de los datos deberá facilitar a las personas afectadas los mecanismos adecuados para ejercer su derecho de acceso, cuando proceda, tanto a las imágenes originales como a las plantillas generadas en el contexto del reconocimiento facial.

Hecho en Bruselas, el 22 de marzo de 2012.

Por el Grupo de trabajo
El Presidente
Jacob KOHNSTAMM