44˚ Sesión Cerrada de la Asamblea Global de Privacidad

Octubre de 2022

Resolución sobre los Principios y Expectativas para el Uso adecuado de la Información personal en la Tecnología de Reconocimiento Facial

Los patrocinadores presentan esta Resolución en nombre del Grupo de Trabajo de Cooperación Internacional para el Cumplimiento de la Ley y del Grupo de Trabajo de Ética y Protección de Datos en la Inteligencia Artificial.

PATROCINADORES:

- Supervisor Europeo de Protección de Datos, Unión Europea
- Comisionado Federal de Protección de Datos e Información, Suiza
- Comisionado de Información y Privacidad, Ontario (Canadá)
- Oficina del Comisionado de Información, Reino Unido
- Oficina del Comisionado de Información de Australia, Australia
- Oficina del Comisionado de Privacidad, Canadá
- Comisión de Protección de la Información Personal, Japón

COPATROCINADORES:

- Autoridad Catalana de Protección de Datos, Cataluña
- Comisión de Informática y Libertades, Burkina Faso
- Autoridad de Protección de Datos, Países Bajos
- Autoridad de Protección de Datos, Noruega
- Autoridad Reguladora de Gibraltar, Gibraltar
- Comisión de Acceso a la Información, Quebec (Canadá)
- Oficina del Comisionado de Información de Jersey, Jersey
- Agencia Nacional de Acceso a la Información Pública, Argentina
- Comisión Nacional de Informática y Libertades, Francia
- Comisión Nacional de Privacidad, Filipinas
- Oficina del Comisionado de Información y Privacidad, Terranova y Labrador (Canadá)
- Oficina del Comisionado de Información y Privacidad, Nueva Escocia (Canadá)
- Oficina del Comisionado de Privacidad, Nueva Zelanda
- Comisión de Protección de la Información Personal, Corea
- Superintendencia de Industria y Comercio, Colombia
- Unidad de Regulación y Control de Datos Personales, Uruguay.

La 44˚ Sesión Anual Cerrada de la Asamblea Global de Privacidad:

Recuerda la Resolución sobre la Tecnología de Reconocimiento Facial (TRF), adoptada en la 42˚ Sesión Cerrada de la Asamblea Global de Privacidad (GPA) en octubre de 2020, que destacó los riesgos para la privacidad de la TRF y encargó al Grupo de Trabajo de Cooperación para el Cumplimiento Internacional (IEWG) y al Grupo de Trabajo de Ética y Protección de Datos en la Inteligencia Artificial (AIWG) que desarrollaran y promovieran un conjunto de principios y expectativas acordados para el uso adecuado de la información personal en la TRF;

Reconoce la creación de un subgrupo de miembros del IEWG y del AIWG y sus esfuerzos para cumplir el mandato establecido en la Resolución sobre la TRF mediante: la realización de investigaciones; la revisión de la literatura; la participación de los miembros de la GPA; la consulta con las partes interesadas globales pertinentes; y el desarrollo de los principios y las expectativas;

Reconoce, tras la adopción de la Resolución sobre TRF en octubre de 2020, el continuo desarrollo e implementación de TRF en vivo y retrospectivas por parte de organizaciones del sector público y privado en una variedad de escenarios como: espacios públicos; lugares de trabajo; tiendas; entornos educativos; en línea; y en zonas de guerra;

Tiene en cuenta el debate global en curso sobre la TRF entre un conjunto diverso de partes interesadas (incluyendo reguladores, legisladores, desarrolladores, usuarios, academia y sociedad civil), y sus respectivas perspectivas sobre los beneficios y riesgos de la TRF, expuestos en resultados de investigación, libros blancos, documentos de posición, opiniones, blogs, artículos de revistas y otras comunicaciones públicas;

Reconoce las importantes contribuciones de las autoridades de protección de datos y privacidad, así como de los organismos internacionales, al debate global, mediante la publicación de documentos de políticas y lineamientos, entre otros:

- las directrices del Consejo Europeo de Protección de Datos sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley, y el dictamen conjunto del SEPD sobre la propuesta de Ley de Inteligencia Artificial de la UE;
- Directrices de privacidad de los Comisionados de privacidad federales, provinciales y territoriales de Canadá sobre el reconocimiento facial para los organismos policiales;
- Marco legal recomendado por los Comisionados de privacidad federales, provinciales y territoriales de Canadá para el uso del reconocimiento facial por parte de las agencias policiales;
- los dictámenes de la Oficina del Comisionado de Información del Reino Unido sobre el uso de la tecnología de reconocimiento facial en lugares públicos y el uso de la tecnología de reconocimiento facial en vivo por parte de las fuerzas del orden en lugares públicos;
- las directrices del Consejo de Europa sobre el reconocimiento facial; y

- Recomendación de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) sobre la ética de la inteligencia artificial.

Destaca las intervenciones reguladoras formales y la actividad de aplicación de las autoridades de protección de datos y privacidad, incluida la realización de investigaciones y la emisión de multas, avisos de aplicación, órdenes de cese y recomendaciones en relación con la implementación de TRF en una variedad de entornos por parte del sector privado, el sector público y los organismos encargados de hacer cumplir la ley.

Tiene en cuenta los reglamentos y desarrollos legislativos existentes que cubren el uso de TRF, incluyendo: la Ley de Privacidad de la Información Biométrica de Illinois, la propuesta de Ley de Inteligencia Artificial de la Unión Europea y la propuesta de Ley de Inteligencia Artificial y Datos de Canadá;

Agradece la aportación de los miembros de la GPA al trabajo del subgrupo de TRF, compartiendo sus perspectivas sobre los riesgos más significativos para la privacidad asociados a usos específicos de TRF;

Acoge la aportación de los usuarios de la TRF, los desarrolladores, los legisladores y las organizaciones de la sociedad civil en el trabajo del subgrupo de la TRF, ayudando a perfeccionar el alcance, la terminología, la claridad, la cobertura y la facilidad de uso de los principios y las expectativas para el uso adecuado de la información personal en la TRF;

Destaca que el cumplimiento de las normas de protección de datos y privacidad es vital para el desarrollo e implementación responsable y fiable de las TRF, en cualquier parte del mundo;

Reitera los compromisos del Plan Estratégico 2021-23 de la GPA para mejorar la voz de la Asamblea en la política digital, fortalecer la cooperación regulatoria y trabajar hacia un entorno regulatorio con altos estándares de protección de datos y privacidad que se apliquen de manera clara y consistente en todo el mundo;

Reconoce que la necesidad de contar con normas mundiales claras y coherentes en materia de protección de datos y privacidad es especialmente importante en el contexto de las innovaciones tecnológicas complejas y de alto riesgo, como la TRF, en el que se pueden obtener beneficios, y las diferencias en la regulación pueden generar incertidumbre para las partes interesadas;

Por lo tanto, **la 44° Asamblea Mundial de Privacidad** respalda los principios y las expectativas para el uso adecuado de la información personal en la tecnología de reconocimiento facial, que se resumen aquí y se proporcionan en su totalidad en el anexo:

1. **FUNDAMENTO LEGAL**: Las organizaciones que utilizan el reconocimiento facial deben tener un fundamento legal claro para la recopilación y el uso de datos biométricos.

2. **RAZONABILIDAD, NECESIDAD Y PROPORCIONALIDAD:** Las organizaciones deben establecer la razonabilidad, necesidad y proporcionalidad del uso de la tecnología de reconocimiento facial y ser capaces de demostrar la aplicación de dichos principios.

3. **PROTECCIÓN DE LOS DERECHOS HUMANOS:** Las organizaciones deben, en particular, evaluar y proteger contra la interferencia ilegal o arbitraria de la privacidad y otros derechos humanos.

4. **TRANSPARENCIA:** El uso del reconocimiento facial debe ser transparente para las personas y grupos afectados.

5. **RENDICIÓN DE CUENTAS:** El uso del reconocimiento facial debe incluir mecanismos claros y eficaces de rendición de cuentas.

6. **PRINCIPIOS DE PROTECCIÓN DE DATOS:** El uso del reconocimiento facial debe respetar todos los principios de protección de datos, incluidos los mencionados anteriormente.

La 44 °Asamblea Global de Privacidad resuelve trabajar juntos en 2022-23 para:

1. Seguir cumpliendo el mandato de la Resolución 2020 de la GPA sobre la TRF desarrollando y aplicando un plan de compromiso para:

    a. promover los principios con una serie de grupos clave de interesados externos; y

    b. evaluar y revisar la aplicación en el mundo real de los principios por parte de los desarrolladores y usuarios de TRF.

2. Pedir que el IEWG y el AIWG continúen trabajando juntos para llevar a cabo esta actividad, y que informen en la 45° Sesión Cerrada de la Asamblea Global de Privacidad sobre sus progresos.

Anexo:

Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology

Global Privacy Assembly

GPA
Global Privacy Assembly

Introducción

En la 42° Sesión Cerrada de la Asamblea Global de Privacidad (GPA) en octubre de 2020, los miembros de la GPA adoptaron una resolución sobre la tecnología de reconocimiento facial (en lo sucesivo, la Resolución).

La resolución reconocía que las posibles aplicaciones de la tecnología de reconocimiento facial podrían aportar beneficios a la seguridad y la protección pública, pero también destacaba que la tecnología tiene la capacidad de permitir una vigilancia arbitraria o ilegal y el potencial de ser muy intrusiva, proporcionar resultados sesgados y menoscabar la protección de datos, la privacidad y los derechos humanos.

Los organismos públicos, las organizaciones privadas y la sociedad civil han expresado su preocupación por el hecho de que la tecnología de reconocimiento facial plantea desafíos de privacidad, legales y éticos que deben ser abordados. Al mismo tiempo, la GPA ha identificado previamente la necesidad de trabajar hacia una política, normas y modelos globales para asuntos de importante impacto en la privacidad. Esto permite un mayor nivel de cooperación reguladora, mejora la prevención, detección y remediación eficientes de los problemas de protección de datos y privacidad, y garantiza la coherencia y la claridad en el sistema de supervisión de la economía digital.

Por tanto, la GPA resolvió desarrollar un conjunto de principios y expectativas acordadas para el uso apropiado de la información personal en la tecnología de reconocimiento facial, incluyendo la recomendación de cómo se pueden mitigar los riesgos. El presente documento sirve a ese propósito.

Acerca del reconocimiento facial

El reconocimiento facial es un proceso en el que las herramientas de software analizan una imagen digital del rostro de una persona, extraen sus rasgos distintivos en una plantilla biométrica y comparan esa plantilla con una o más plantillas biométricas extraídas previamente. Esto puede hacerse con fines de **verificación** (por ejemplo, una comparación uno a uno para verificar una reclamación de identidad presentada por una persona) o de **identificación** (por ejemplo, una comparación uno a muchos o muchos a muchos de una imagen de una persona desconocida con respecto a una base de datos de referencias biométricas). Puede ocurrir en una variedad de modos, incluyendo aplicaciones **en vivo** o **casi en vivo** (por ejemplo, la comparación en tiempo real de una o más caras contra una lista de vigilancia) y aplicaciones **retrospectivas** (por ejemplo**,** la comparación de una imagen previamente capturada de una persona reconocida con respecto a una base de datos de referencias biométricas, como sucede durante una investigación policial).

Como se reconoce en la Resolución, la tecnología de reconocimiento facial se basa en información biométrica sensible que es única para la persona y difícil de alterar. Las decisiones que se toman sobre las personas utilizando estos identificadores, a menudo sin su conocimiento o consentimiento, pueden tener consecuencias adversas sin vías de recurso adecuadas. Además de las repercusiones en la privacidad, el uso generalizado del reconocimiento facial también puede tener efectos discriminatorios y afectar a la capacidad

de ejercer otros derechos humanos fundamentales, como la libertad de expresión, movimiento y asociación.

Aplicación de los principios

Estos principios se aplican a todos los tipos y usos del reconocimiento facial por parte de organizaciones tanto del sector privado como del público (incluidas las fuerzas del orden). Aunque para facilitar la referencia hemos utilizado el término "reconocimiento facial" en todo el documento, los principios expuestos a continuación se aplican igualmente a cualquier análisis biométrico de imágenes faciales y plantillas biométricas (como la inferencia de características demográficas, estado emocional, etc.). Los principios pretenden aplicarse a los usuarios, desarrolladores y proveedores de sistemas de reconocimiento facial.

Es importante destacar que los principios que se exponen a continuación tienen una importancia equivalente y deben considerarse de forma global.

Por último, reconocemos que los gobiernos y los reguladores de la protección de datos tienen un papel importante en la tecnología de reconocimiento facial, especialmente en lo que respecta al establecimiento y la aplicación de marcos normativos adecuados. Sin embargo, esto queda fuera del ámbito de este documento.

Terminología

En este documento hemos utilizado los siguientes términos:

> **Biometría**: Una biometría es la medición de una característica fisiológica (por ejemplo, la huella dactilar, el iris, el rostro o la geometría de la mano de una persona) o un atributo de comportamiento (por ejemplo, el modo de andar o el patrón de pulsación de teclas) de una persona. Estas características son, en su mayoría, persistentes, únicas para cada persona, y difíciles o imposibles de cambiar (es decir, cambiar una biometría requiere un cambio en la persona física de la persona). Por ello, deben considerarse información sensible.
>
> **Plantilla biométrica**: Representación digital o matemática de la biometría de una persona. Aunque el formato específico de la plantilla es modificable, representa una característica que es única, difícil de alterar y está inseparablemente ligada a una persona; como tal, debe ser tratada como información sensible.
>
> **Sonda biométrica**: Plantilla biométrica extraída de una imagen de una persona desconocida o no verificada, que se comparará con una referencia biométrica (en el caso de la verificación) o con una base de datos de referencia (en el caso de la identificación).
>
> **Referencia biométrica**: Plantilla biométrica extraída de una imagen asociada a una identidad conocida, con la que se compara una sonda biométrica.
>
> **Base de datos de referencia**: Lista o base de datos de referencias biométricas, con respecto a cada una de las cuales se compara una sonda biométrica.

Consideraciones legales

Los principios que figuran a continuación están redactados como recomendaciones (utilizando el término "debería"). Sin embargo, muchos de ellos son requisitos legales explícitos en las jurisdicciones de los miembros o pueden ser interpretados como tales por los tribunales y las autoridades de protección de datos. Corresponde a cualquier organización que desee utilizar la tecnología de reconocimiento facial comprender los obligaciones legales aplicables en su jurisdicción.

PRINCIPIOS

1. FUNDAMENTO LEGAL: Las organizaciones que utilizan el reconocimiento facial deben tener un fundamento legal claro para la recopilación y el uso de datos biométricos.

1.1. Las organizaciones deben documentar la legalidad del uso de la biometría para el reconocimiento facial y estar preparadas para demostrar dichos principios. Esto incluye tanto el fundamento legal para capturar una imagen de una persona para crear una sonda biométrica, como para crear, acceder o modificar cualquier base de datos de referencia que se utilice o vaya a utilizarse. Esto debería reevaluarse periódicamente para tener en cuenta los cambios en la legislación o su interpretación.

1.2. Si operan en una jurisdicción que reconoce diversos fundamentos legales para el tratamiento de datos, las organizaciones deben considerar si otra base es más apropiada que el consentimiento. En muchas aplicaciones, incluido el uso del reconocimiento facial en espacios de acceso público y en contextos laborales, puede resultar difícil para una organización demostrar que ha obtenido un consentimiento significativo de una persona.

1.3. Si el consentimiento es la base del tratamiento de datos, las organizaciones deben garantizar y poder demostrar que el consentimiento es significativo. Esto significa que es informado, específico, actual, dado libremente y sin ambigüedades. Esto incluye la consideración de la capacidad de la persona para dar un consentimiento significativo (como en el caso de los jóvenes o las personas vulnerables).

> 1.3.1. Es preferible el consentimiento expreso. Las organizaciones deben ser conscientes de que el consentimiento implícito no cumpliría la norma de consentimiento en muchas jurisdicciones y, en general, no debe confiarse en él para la recopilación de información personal sensible. Sin embargo, si una organización considera que puede confiar en el consentimiento implícito para el reconocimiento facial, debe ser capaz de demostrar que es (i) apropiado en las circunstancias, y (ii) razonable creer en las circunstancias en que una persona ha dado su consentimiento.

1.4. Las organizaciones deben ser conscientes de que, en muchas jurisdicciones, la extracción de imágenes de plataformas en línea de acceso público (incluidas las de los servicios de redes

sociales) para crear una base de datos de referencia de reconocimiento facial no se considera lícito ni justo, ni tampoco un proceso transparente.

2. RAZONABILIDAD, NECESIDAD Y PROPORCIONALIDAD: Las organizaciones deben establecer, y ser capaces de demostrar, la razonabilidad, necesidad y proporcionalidad de su uso de la tecnología de reconocimiento facial.

2.1. Las organizaciones deben establecer la necesidad de utilizar la tecnología de reconocimiento facial. Dada la sensibilidad de la información en cuestión, el umbral para establecer la necesidad es alto. Requiere que se establezca claramente la finalidad prevista, que la tecnología de reconocimiento facial pueda ser eficaz para lograr esta finalidad y que la finalidad no pueda lograrse razonablemente por medios menos intrusivos. No se deben invocar la conveniencia o la utilidad para establecer la necesidad.

2.2. Las organizaciones deben establecer, y ser capaces de demostrar, la proporcionalidad de su uso de la tecnología de reconocimiento facial. De nuevo, el umbral para establecer la proporcionalidad es alto. Los beneficios del uso del reconocimiento facial deben superar claramente el riesgo de daño que supone para la privacidad de las personas y otros derechos humanos. Al establecer la proporcionalidad:

> 2.2.1. Las organizaciones deben documentar los beneficios esperados del uso de la tecnología de reconocimiento facial y ser capaces de comprobarlos. Las organizaciones también deben definir claramente cómo van a medir si el sistema ha obtenido estos beneficios, y el nivel de beneficio por debajo del cual se dejaría de utilizar el reconocimiento facial.
>
> 2.2.2. Las organizaciones deben documentar que han evaluado los riesgos potenciales o conocidos de daño que supone el uso propuesto del reconocimiento facial y ser capaces de demostrarlos. Esto debería incluir la consideración de los riesgos de daño a las personas y a los grupos. Las organizaciones también deben documentar claramente las medidas que han aplicado para mitigar los riesgos identificados.
>
> 2.2.3. En el caso de la identificación, una organización debe demostrar un claro interés público en el uso de la tecnología. En general, el beneficio comercial no se considerará por sí mismo un interés público claro.
>
> 2.2.4. El umbral de proporcionalidad puede cumplirse más fácilmente en los casos de uso de la tecnología de reconocimiento facial para la verificación cuando la organización pueda demostrar que las personas han consentido de forma significativa el uso del sistema, tal como se establece en el principio 1.3.

2.3. Las organizaciones deben establecer la razonabilidad de su uso de la tecnología de reconocimiento facial. El umbral para establecer la razonabilidad es alto. Lo que es razonable es una cuestión de hecho en cada caso particular. La razonabilidad puede verse influida por las expectativas de la comunidad, así como por las normas y prácticas actuales de la tecnología de reconocimiento facial.

2.4. Para evitar que en las decisiones influyan costos o compromisos irrecuperables, la evaluación de la razonabilidad, la necesidad y la proporcionalidad debe realizarse antes de la compra, el desarrollo o la implementación de un sistema de reconocimiento facial.

2.5. Las organizaciones deben ser conscientes de cualquier determinación de sus respectivas autoridades de protección de datos de que los daños conocidos o potenciales de determinadas aplicaciones del reconocimiento facial son tan importantes que no pueden ser proporcionales a los beneficios previstos.

> 2.5.1. En particular, las organizaciones deben ser conscientes de que el daño potencial asociado al reconocimiento de los rasgos humanos en espacios de acceso público (incluido el reconocimiento facial) ha llevado a múltiples autoridades de protección de datos nacionales, regionales y locales, incluidas todas las autoridades de protección de datos del EEE, a proponer prohibiciones de esta práctica.
>
> 2.5.2. Las organizaciones también deben ser conscientes de que muchas autoridades de protección de datos han pedido que se prohíban otras formas de análisis facial no relacionadas con la verificación e identificación, como la inferencia del estado emocional.

2.6. La evaluación de la organización sobre la razonabilidad, la necesidad y la proporcionalidad debe revisarse periódicamente. Esto debería considerar, entre otros criterios, si persiste la necesidad que se aborda; si se han obtenido los beneficios esperados del uso del reconocimiento facial; y si han surgido daños no identificados previamente, o si los daños identificados han sido peores de lo previsto, de manera que esos daños ahora superan los beneficios.

3. PROTECCIÓN DE LOS DERECHOS HUMANOS: Las organizaciones deben, en particular, evaluar y proteger contra la interferencia ilegal o arbitraria de la privacidad y otros derechos humanos.

3.1. En general, las organizaciones deben asumir que el uso de la tecnología de reconocimiento facial puede interferir indebidamente con los derechos de protección de datos y privacidad de las personas.

> 3.1.1. Esta interferencia suele ser mayor cuando se utilizan estas tecnologías en un espacio de acceso público. Las organizaciones deben tener especialmente en cuenta que la presencia de una persona en un lugar público no significa necesariamente que haya renunciado a cualquier expectativa razonable de privacidad o control de la información personal. De acuerdo con el principio 2.5.1, diversas autoridades de protección de datos han propuesto prohibir tales usos.
>
> 3.1.2. Las interferencias también aumentarán debido a cualquier aplicación del reconocimiento facial que rastree los movimientos, acciones o comportamientos de una persona a lo largo del tiempo (en el mismo o en múltiples lugares y, en particular, en lugares que puedan revelar información sensible sobre una persona).

3.2. Las organizaciones no deben suponer que las imágenes de personas que son accesibles públicamente en Internet (incluidos los sitios de medios sociales) pueden ser recopiladas y transformadas para su uso como sondas biométricas o referencias biométricas, o para entrenar un sistema de reconocimiento facial, sin el conocimiento y el consentimiento de esas personas u otro fundamento legal para dicha recopilación y uso.

3.3. A la hora de determinar los posibles impactos sobre la protección de datos y el derecho a la intimidad, las organizaciones deberían:

3.3.1. Llevar a cabo las evaluaciones de impacto adecuadas (como una evaluación de impacto sobre la privacidad, una evaluación de impacto sobre la protección de datos o una evaluación de impacto sobre los derechos humanos).

3.3.1.1. Las organizaciones deben ser transparentes con todas las personas potencialmente afectadas sobre su evaluación y mitigación de los riesgos para la privacidad.

3.3.2. Considerar las diferencias demográficas (es decir, el sesgo) con respecto tanto al funcionamiento del sistema (por ejemplo, las diferencias de rendimiento relevantes entre los grupos) como a la aplicación del sistema (por ejemplo, las diferencias en la forma en que la implementación del sistema afectará a las personas o grupos). Las organizaciones también deben considerar cómo van a medir, de forma continua, cualquier impacto diferencial entre grupos del uso del sistema de reconocimiento facial.

3.3.3. Considerar el posible "efecto amedrentador" sobre derechos como la libertad de expresión y la libertad de asociación, así como el potencial de discriminación, relacionado con el uso de sistemas de reconocimiento facial en espacios de acceso público, independientemente de la finalidad prevista de dichos sistemas.

3.3.4. Cuando los grupos marginados puedan verse afectados especialmente por el uso de un sistema, consultar con los representantes de esos grupos sobre los impactos previstos y las estrategias para reducir los daños.

3.4. En la medida de lo posible, cuando se utilice el reconocimiento facial para la verificación, deberá ofrecerse un método alternativo que no se base en la biometría, incluso para aquellas personas que rechacen o retiren su consentimiento. Ninguna persona deberían se penalizada por el uso de esta alternativa.

4. TRANSPARENCIA: El uso del reconocimiento facial debe ser transparente para las personas y grupos afectados.

4.1. Las organizaciones deben garantizar que las personas reciban información(en un lenguaje sencillo) de:

4.1.1. En cualquier momento en que su imagen facial capturada se someta a un sistema de reconocimiento facial, o que su plantilla biométrica se incluya en una base de datos de referencia para un sistema de reconocimiento facial. Es preferible y

constituye una buena práctica -y en algunas circunstancias, es obligatorio por ley- que se notifique a las personas antes o en el momento en que se capture su imagen facial.

4.1.2. Sus derechos sobre los datos con respecto a los sistemas de reconocimiento facial, así como la forma de ejercerlos. Esto incluye, entre otros, la posibilidad de solicitar que su imagen facial no se someta a un sistema de reconocimiento facial, que su plantilla biométrica se elimine de una base de datos de referencia (si procede) o que se corrija la información sobre ellos en un sistema de reconocimiento facial (por ejemplo, actualizando su referencia biométrica).

4.1.3. Cualquier otra información que deba proporcionarse a las personas por ley en su jurisdicción. Esto incluye cómo y dónde se almacenará la información, con qué fines se tratará, cuánto tiempo se conservará y con qué organizaciones puede compartirse.

4.2. Las organizaciones deben considerar cómo se asegurarán de que se proporciona una notificación adecuada a todas las personas, incluidos los jóvenes y las personas vulnerables.

4.3. Las organizaciones deben ser conscientes de que la señalización sobre el uso de un sistema de reconocimiento facial generalmente no será suficiente, por sí sola, para el cumplimiento del Principio 4.1.

4.3.1. Cuando el tratamiento se base en el consentimiento, y la señalización sea un elemento de este proceso de consentimiento, la señalización deberá estar bien visible antes de que una persona entre en una zona vigilada. Esta señalización debe incluir una indicación de las alternativas disponibles para acceder al espacio. La señalización también debe indicar claramente que se está utilizando el reconocimiento facial, a diferencia de una cámara de seguridad estándar.

4.3.2. Cuando la señalización sea una parte fundamental de la estrategia de aviso de una organización, se debe considerar cómo se avisará a aquellos que puedan tener dificultades para leer o entender las señales.

4.4. En el caso del reconocimiento facial retrospectivo, las organizaciones deben tomar medidas proactivas para garantizar que las personas sean conscientes del uso y la finalidad del sistema. Esto incluye tanto la publicación de esta información antes de la utilización del sistema, como (siempre que sea razonable) la notificación específica a las personas cuyas imágenes han sido procesadas por el sistema.

5. RENDICIÓN DE CUENTAS: El uso del reconocimiento facial debe incluir mecanismos claros y eficaces de rendición de cuentas.

5.1. Las organizaciones deben establecer políticas claras de gobernanza y mitigación de riesgos para todos los usos del reconocimiento facial y estar preparadas para demostrar la existencia y eficacia de estas políticas.

5.1.1. Las organizaciones deben establecer y mantener un medio para detectar el incumplimiento de las políticas de gobernanza y gestión de riesgos para el

reconocimiento facial (incluso por parte de actores internos), y las consecuencias del incumplimiento.

5.2. Todos los usuarios de un sistema de reconocimiento facial deben recibir una formación periódica sobre las políticas internas de privacidad pertinentes, los requisitos legales de su jurisdicción, las limitaciones y los posibles sesgos de los sistemas de reconocimiento facial, cómo realizar la comparación facial y las formas de mitigar los riesgos conocidos, como el sesgo de automatización (es decir, la tendencia de los humanos a dar mayor peso a las sugerencias realizadas por un sistema automatizado).

5.3. Siempre que sea razonable, las conclusiones a las que se llegue sobre la identidad de una persona deben ser evaluadas por una persona que haya recibido la formación pertinente. Este es el caso, en particular, cuando una persona se vea afectada de forma significativa por dicha conclusión.

5.3.1. Las personas deben tener la oportunidad de impugnar cualquier decisión tomada sobre ellas basada en una identificación mediante reconocimiento facial y de solicitar una reparación.

5.3.2. Las organizaciones deben asegurarse de que el umbral de "coincidencia" es razonable para la aplicación propuesta del sistema, ya sea que este umbral sea determinado por la propia organización o por el desarrollador del sistema.

5.3.3. Las organizaciones deben establecer estrategias de mitigación para gestionar los riesgos asociados a las discordancias (tanto falsos positivos como falsos negativos) y a los registros erróneos (es decir, inexactitudes en la base de datos de referencia).

5.4. Las organizaciones deben reconocer las limitaciones de los sistemas de reconocimiento facial e interpretar los resultados producidos por dichos sistemas en consecuencia. Por ejemplo, en el contexto de un sistema de reconocimiento facial retrospectivo utilizado por las fuerzas de seguridad, una "coincidencia" debe considerarse una pista potencial en lugar de una prueba concluyente o admisible.

5.5. Las organizaciones deben realizar auditorías periódicas sobre la eficacia del sistema de reconocimiento facial, las medidas de mitigación de riesgos establecidas y el cumplimiento interno de las políticas de gobernanza.

5.6. Las organizaciones deben controlar y evaluar periódicamente cualquier diferencia demográfica en la eficacia de su uso de un sistema de reconocimiento facial.

5.7. Las organizaciones que desarrollen sistemas de reconocimiento facial deberán documentar las medidas adoptadas para medir y proteger contra las diferencias demográficas en sus productos, así como la eficacia de estas medidas (es decir, cualquier diferencia de rendimiento conocida entre grupos demográficos).

5.8. Las organizaciones que deseen adquirir o utilizar de algún modo sistemas de reconocimiento facial deberán:

5.8.1. Obtener información sobre la medición y la protección de las diferencias demográficas documentadas según el principio 5.7.

5.8.2. Obtener información sobre la demografía de los conjuntos de datos de formación, prueba y evaluación del producto, para asegurarse de que han incluido una gama de personas suficientemente diversa para el contexto previsto.

5.8.3. Asegurarse de que el producto ha sido diseñado y probado de forma compatible con el uso previsto. Por ejemplo, un producto de reconocimiento facial diseñado para la verificación en un entorno bien iluminado y controlado puede no ser lo suficientemente preciso para la identificación en un entorno oscuro, de gran ángulo o muy dinámico (es decir, una multitud en movimiento).

5.8.4. Si se recurre a un proveedor de servicios externo, contar con un marco sólido de gestión de riesgos del proveedor para evaluar el cumplimiento del principio 5.10, así como con las protecciones contractuales asociadas para garantizar el cumplimiento continuo.

5.9. Las organizaciones deben establecer procedimientos y políticas para identificar, mitigar, responder y notificar a la autoridad de protección de datos pertinente cualquier violación de datos relacionada con el sistema de reconocimiento facial.

5.10. Las organizaciones deben asegurarse de que los terceros que contraten cumplan con los Principios establecidos en este documento (en la medida en que se apliquen al tercero), así como con cualquier requisito legislativo.

6. PRINCIPIOS DE PROTECCIÓN DE DATOS: El uso del reconocimiento facial debe respetar todos los principios de protección de datos, incluidos los mencionados anteriormente.

Las organizaciones deben tener en cuenta *todos los* principios de protección de datos a lo largo del ciclo de vida de un sistema de reconocimiento facial. Además de los descritos anteriormente, estos incluyen:

6.1. Privacidad por diseño.

6.1.1. Al desarrollar un sistema de reconocimiento facial, las organizaciones deben adoptar un enfoque de privacidad por diseño para garantizar que las protecciones se incorporen a los sistemas de reconocimiento facial desde el principio.

6.1.2. Cuando sea razonable, las organizaciones deberían evitar el almacenamiento central de plantillas biométricas y de cualquier dato biométrico en bruto. Por ejemplo, en el caso de la verificación, la referencia biométrica podría almacenarse en un dispositivo o artefacto (como un permiso de conducir, un pasaporte o una tarjeta de identificación de empleado) en posesión de la persona que está siendo verificada. Si las plantillas biométricas se almacenan de forma centralizada (cuando se identifiquen los fines específicos para ello), deberían estar protegidas por medidas criptográficas fuertes y adecuadas.

6.1.3. Las organizaciones que utilicen un sistema de reconocimiento facial deben asegurarse de que se aplican las garantías adecuadas a lo largo de cada etapa del ciclo de vida de la información del sistema.

6.2. Especificación de la finalidad y limitación del uso**.**

6.2.1. Las organizaciones deben definir claramente los fines para los que se utilizarán los sistemas de reconocimiento facial, y no variar dichos fines a menos que esté legalmente permitido.

6.3. Minimización, retención y eliminación de datos.

6.3.1. Las organizaciones deben definir períodos de conservación para los datos biométricos brutos y las plantillas biométricas (incluidas las utilizadas como sondas biométricas o referencias biométricas, o almacenadas en bases de datos de referencia), y eliminar las plantillas biométricas cuando ya no sea necesario conservarlas. Este periodo debería tener en cuenta la utilidad decreciente de una plantilla biométrica con el paso del tiempo.

6.3.2. En general, las sondas biométricas que no coincidan con una referencia biométrica deberán eliminarse inmediatamente. La conservación limitada de dichas imágenes puede ser aceptable si es razonablemente necesaria, como por ejemplo para la comprobación del sistema, que tiene una base jurídica clara y está en consonancia con la finalidad definida para el tratamiento en cuestión, cuando existe una política de conservación adecuada. Las sondas biométricas coincidentes pueden conservarse durante un período determinado, pero sólo deben utilizarse en relación con esa coincidencia (es decir, con fines probatorios, o para permitir a las personas impugnar una decisión tomada al respecto).

6.3.3. A menos que sea necesario para un propósito definido (y legal), las organizaciones deben evitar crear un perfil de las actividades o comportamientos de una persona mediante la correlación de las coincidencias de reconocimiento facial a través del tiempo.

6.3.4. Las organizaciones deben disponer de mecanismos accesibles para que las personas puedan solicitar la eliminación de su plantilla biométrica de una base de datos de referencia cuando ya no consientan su inclusión, o tengan otros motivos legales para solicitar y obtener la eliminación. Dichas supresiones deben ser rápidas y tener lugar lo antes posible (y dentro de los plazos legalmente definidos).

6.4. Garantías.

6.4.1. Las organizaciones deben aplicar garantías de seguridad proporcionales a la alta sensibilidad de la información en un sistema de reconocimiento facial.

6.4.2. Las organizaciones deben aplicar las políticas, los procedimientos, las normas de seguridad y los controles necesarios para garantizar que ni el sistema de reconocimiento facial ni la información personal que recopila o almacena sean objeto de acceso no autorizado o no intencionado, uso indebido, interferencia o pérdida.

6.4.3. Las organizaciones deben asegurarse de que todos los sistemas de reconocimiento facial que estén desplegando (incluidos los desarrollados por terceros) incluyan medidas adecuadas de protección de plantillas biométricas, y que estas protecciones estén en uso. En la medida de lo posible, éstas deberían ajustarse a las normas reconocidas internacionalmente para la protección de la información biométrica.

6.4.4. Las organizaciones deben revisar periódicamente sus garantías de seguridad para asegurarse de que siguen siendo suficientes para un panorama de amenazas en evolución.

6.5. Calidad de los datos.

6.5.1. Las organizaciones deben asegurarse de que las referencias biométricas, y cualquier otra información personal recopilada, generada y almacenada por el sistema de reconocimiento facial, sean lo suficientemente precisas y estén actualizadas para los fines para los que se utilizan.

6.5.2. Las organizaciones deben tomar medidas razonables para corregir o eliminar cualquier información personal que sea inexacta en relación con los fines para los que se utiliza.

6.5.3. Las organizaciones deben asegurarse de que sólo se incluyan en las bases de datos biométricos de referencia o se utilicen como sondas biométricas las imágenes adecuadas para su uso con sistemas de reconocimiento facial. Las evaluaciones de calidad deben tener en cuenta, como mínimo, las características de la imagen, incluyendo la pose, la iluminación, la expresión, el tamaño y la resolución de la imagen y la oclusión facial (es decir, la presencia de gafas, sombreros, pañuelos o máscaras).