14 equívocos con relación a la identificación y autenticación biométrica

Junio 2020

www.aepd.es/es
www.edps.europa.eu

La identificación es el proceso de reconocer a un individuo particular entre un grupo. Este proceso compara los datos del individuo a identificar con los datos de cada individuo en el grupo. La autenticación es el proceso de probar que es cierta la identidad reclamada por un individuo. Este proceso compara los datos del individuo únicamente con los datos asociados a la identidad reclamada.

En paralelo a la reciente popularización del uso de datos biométricos para fines de identificación y autenticación (por ejemplo, huellas dactilares o mediciones faciales) se han extendido una serie de equívocos con relación a esta tecnología. Este documento enumera catorce de ellos, explica su fundamento y proporciona referencias científicas que respaldan las aclaraciones.

1. "La información biométrica se almacena en un algoritmo"

Un algoritmo (RAE) es un método, un conjunto ordenado de operaciones o una receta y no un medio para almacenar datos biométricos.

La información biométrica recogida (por ejemplo, la imagen de una huella dactilar) se procesa siguiendo procedimientos definidos en estándares[1] y el resultado de ese proceso se almacena en registros de datos denominados firmas, patrones o "*templates*". Estos patrones registran numéricamente las características físicas que permiten diferenciar personas.

Por otro lado, hay que señalar que para algunos tratamientos de identificación y autenticación existen soluciones implementados con técnicas de Machine Learning que contienen, en la propia aplicación y accesibles, parte de los datos biométricos utilizados para su desarrollo[2].

2. "El uso de datos biométricos es igual de intrusivo que cualquier otro sistema de identificación/autenticación"

A diferencia de una contraseña o un certificado, los datos biométricos recogidos durante un procedimiento de autenticación o identificación revela más información personal sobre el sujeto. Dependiendo de los datos biométricos recogidos, pueden derivarse datos del sujeto como su raza o género (incluso de las huellas dactilares[3]), su estado emocional, enfermedades, discapacidades y características genéticas, consumos de sustancias, etc[4]. Al estar implícita, el usuario no puede impedir la recogida de dicha información suplementaria.

[1] En la página 2 se puede ver el formato de datos de huella digitalizada ISO 19794-2: https://www.ekds.gov.tr/bio/FM3_README.pdf
Un ejemplo mucho más extenso para firma manuscrita: https://e-archivo.uc3m.es/bitstream/handle/10016/10990/PFC_Roberto_Pizarro_Santos.pdf?sequence=1&isAllowed=y

[2] Machine Learning Models that Remember Too Much: https://arxiv.org/pdf/1709.07886.pdf

[3] Información que es posible extraer de una huella dactilar: https://www.scientificamerican.com/article/the-hidden-data-in-your-fingerprints/

[4] Biometría-Soft es el campo de estudio de carácteristicas no únicas del individuo a partir de su información biométrica, como estado mental, salud, etc. Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data.
IET Biometrics https://digital-library.theiet.org/docserver/fulltext/iet-bmt/6/6/IET-BMT.2016.0169.pdf?expires=1588324856&id=id&accname=guest&checksum=FC6EA4A19D569EC51629E68254BB0884

agencia española protección datos

EDPS
European Data Protection Supervisor

3. "La identificación/ autenticación biométrica es precisa"

A diferencia de los procesos basados en contraseñas o certificados, que es 100% precisa (p. ej. una clave puede ser correcta o no serlo), la identificación/autenticación biométrica se basa en probabilidades (p. ej. una huella digitalizada proporcionará una correspondencia al 96% con un individuo). Existe una determinada tasa de falsos positivos (da por buena una suplantación) y falsos negativos (rechaza a un individuo autorizado).

Estas tasas son mayores cuanto menos preciso sea el equipo de captura de datos[5] y dependen de las condiciones de recogida (p. ej. la luminosidad o limpieza del sensor). La precisión de algunos datos biométricos, como las huellas dactilares, también depende de la edad del individuo y es afectada por su envejecimiento[6].

4. "La identificación/ autenticación biométrica es suficientemente precisa para diferenciar siempre entre dos personas"

Está demostrado que el parecido biométrico entre hermanos o familiares ha confundido a sistemas biométricos[7]. En particular, la identidad de patrones biométricos para la identificación de hermanos gemelos más allá del reconocimiento facial es un campo de estudio[8]. Es más, las condiciones medioambientales en entornos no controlados (i.e., reconocimiento facial en espacios públicos, el uso de con pintura facial o máscaras antivirales) provoca el aumento de la tasa de error y por tanto que la confusión sea más probable.

5. "La identificación/ autenticación biométrica es adecuada para todas las personas"

Algunas personas no pueden utilizar determinados tipos de biometría porque sus características físicas no son reconocidas por el sistema. En casos de lesiones, accidentes, problemas de salud (como parálisis) y otros, la incompatibilidad puede ser temporal. La incompatibilidad biométrica permanente puede ser una causa de exclusión social[9].

6. "El proceso de identificación/autenticación biométrica no se puede burlar"

Existen procedimientos y técnicas que permiten burlar sistemas de autenticación biométrica y asumir la identidad de otra persona.

Algunos de esos medios, como el uso de máscaras[10] o de reproducciones de la huella[11] no

[5] Pobre rendimiento de los sistema de reconocimiento facial de la policía británica: https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure

[6] Sobre la degración de la calidad de la información recogida de personas según se envejece: https://www.researchgate.net/publication/328526153_A_Study_of_Age_and_Ageing_in_Fingerprint_Biometrics

[7] Burla del reconocimiento facial: https://www.ipadizate.es/2017/11/04/hermanos-burlan-face-id-iphone-x/

[8] Biometric Identification of Identical Twins: A Survey. Conference: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). https://www3.nd.edu/~kwb/Bowyer_Flynn_BTAS_2016.pdf

[9] Riesgos de exclusión social de los sistemas biométricos de la tarjeta ID británica: https://privacyinternational.org/sites/default/files/2017-12/UK%20Identity%20Cards.pdf

[10] Una máscara de US$200 burla el Face ID del iPhone X https://www.cnet.com/es/noticias/mascara-200-dolares-burla-face-id-del-iphone-x/

[11] Estudiantes que burlan el sistema de identificación de huella de su centro: https://www.hindustantimes.com/mumbai-news/you-will-be-glued-to-this-mumbai-college-s-students-trick-biometric-system/story-W64f1jdMtecxKDml2DakeI.html

requieren de grandes conocimientos técnicos o recursos económicos. Existen también los denominados "sistemas adversarios", que están diseñados específicamente para tratar de engañar a los sistemas de reconocimiento de imágenes y que pueden utilizarse para burlar la identificación biométrica[12].

7. "La información biométrica no está expuesta"

A diferencia de los procesos basados en contraseñas o certificados, la mayor parte de características biométricas de una persona están expuestas y se pueden capturar a distancia, ya que no se oculta habitualmente el rostro, las huellas, la forma de moverse, la huella térmica, etc.

Por otro lado, aquellos sujetos que quieren burlar activamente los sistemas de seguimiento o identificación biométrica, tienen recursos disponibles para hacerlo[13], lo que no es el caso para la gran mayoría de los ciudadanos.

Si no se toman medidas que reduzcan el riesgo de uso no autorizado de datos biométricos, su uso equivale a llevar escrito en la frente nuestras claves de acceso[14].

8. "Todo tratamiento biométrico implica identificación/autenticación"

No necesariamente. Por ejemplo, el tratamiento biométrico del movimiento del ratón utilizado para determinar si un robot está accediendo a una página web implica tratar la información biométrica para diferenciar humano de máquina. Igualmente, se puede realizar tratamiento biométrico para determinar si en un espacio restringido existe un intruso humano o animal, o en sistemas de digital signage[15] se puede diferenciar un hombre, mujer o niño. Lo que existe es un riesgo de tratar esa información más allá del propósito original en el caso de que, por ejemplo, se produzca un fallo de seguridad, un cambio normativo o un tratamiento ilegítimo.

9. "Los sistemas de identificación/autenticación biométrica son más seguros para los usuarios"

Cualquiera de los múltiples sistemas en los que nuestros datos biométricos estén siendo procesados puede sufrir una brecha de seguridad. El acceso no autorizado a nuestros datos biométricos en un sistema permitiría o facilitaría (en el caso de utilizar múltiples factores de autenticación) el acceso en el resto de los sistemas que utilicen dichos datos biométricos.

Podría tener el mismo efecto que usar la misma contraseña en muchos sistemas distintos, por lo que la escala en la implantación biométrica es un problema en sí mismo. Y, a diferencia de los sistemas basadas en contraseñas, una vez que la información biométrica ha sido comprometida, esta no se puede cancelar.

Si antes la información biométrica se almacenaba en unas pocas bases de datos (principalmente con fines relacionados con la seguridad pública o el control de las fronteras), ahora está almacenada cada vez en más entidades y dispositivos. Eso aumenta

[12] On adversarial patches: real-world attack on ArcFace-100 face recognition systems https://arxiv.org/pdf/1910.07067.pdf

[13] Accesorios para evitar el reconocimiento facial: https://www.businessinsider.com/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10?IR=T#images-from-echizens-lab-shows-how-the-visor-blocks-ais-ability-to-detect-a-face-6

[14] Peligro de exponer las huellas en las fotos que se suben a Internet: https://www.bleepingcomputer.com/news/security/scientists-extract-fingerprints-from-photos-taken-from-up-to-three-meters-away/

[15] Proyectores que emplean tecnologías como LCD, LED, proyección y e-paper para mostrar imágenes digitales, video, páginas web, información meteorológica, menús, o texto.

enormemente la probabilidad de una brecha de seguridad de información biométrica (durante su recogida, transmisión, almacenamiento o proceso), algo que ya está sucediendo[16].

10. "La autenticación biométrica es fuerte"

Por definición, un sistema de autenticación fuerte es aquel que exige que se proporcione, al menos, dos de los siguientes: algo que se sabe, algo que se tiene o algo que se es (biometría).

Por definición, sólo utilizar biometría es un proceso de autenticación débil, mientras que utilizar una tarjeta de acceso y contraseña es fuerte. Aunque la autenticación biométrica muchas veces exige un proceso previo de registro o identificación en el que, por ejemplo, en reconocimiento facial, hay que comparar con la foto en el DNI, si, después del proceso de identificación, el proceso de autenticación sólo es biométrico, sigue siendo un sistema débil.

11. "La identificación/ autenticación biométrica es más cómoda para el usuario"

Esta afirmación depende de la tecnología empleada y de las circunstancias, percepción y cultura de cada usuario. A parte de los problemas de idoneidad descritos en el punto 5, pueden existir otros problemas que afecten negativamente la percepción del usuario: sentimiento de invasión a la privacidad, fallos en los sistemas biométricos que impidan el acceso a los servicios, carencia de alternativas no-biométricas eliminadas o inadecuadas para dar el mismo servicio, así como la necesidad de realizar procesos de registro de datos en cada entidad[17].

12. "La información biométrica convertida a un hash no es recuperable"

Para añadir seguridad al tratamiento de la información biométrica, es recomendable eliminar el patrón biométrico del que se ha obtenido el hash[18] o biohash[19]. Sin embargo, hay estudios que demuestran que el hash puede ser reversible, es decir, podría ser posible obtener el patrón biométrico original, sobre todo si se vulnera el secreto de la clave utilizada para generar el hash[20].

13. "La información biométrica almacenada no permite reconstruir la información biométrica original de la que se ha extraído"

La información biométrica almacenada (p. ej. el patrón) permite reconstruir parcialmente la información biométrica original (p. ej. la cara). Dicha reconstrucción parcial tiene en ocasiones la fidelidad suficiente para que otro sistema biométrico la reconozca como el original. Por ejemplo, en información biométrica facial hay estudios que demuestran que es

[16] Una brecha de seguridad expone millones de registros de huellas y reconocimiento facial recogidas en el sistema financiero: https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#15cedb5f46c6

[17] Caixabank ofrece una cita previa para capturar el reconocimiento facial: https://www.caixabank.es/particular/banca-digital/face-id_es.html#

[18] Una función hash es un proceso que transforma cualquier conjunto de datos (p. ej. una huella digitalizada) en un conjunto de valores de longitud fija. Para más información sobre funciones hash y su uso como técnica de seudonimización consultar: https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf

[19] El biohash es una técnica utilizada para combinar tokens aleatorios con datos biométricos. Para más información consultar: https://www.researchgate.net/publication/234809846_Remarks_on_BioHash_and_its_mathematical_foundation

[20] Modelos de ataque de inversión: https://link.springer.com/article/10.1186/s13634-016-0396-1#Sec5
El patrón se puede obtener de un biohash: https://bit.ly/3gPfNhJ

posible conseguir desde un retrato robot a una representación fiel[21]. La fidelidad de la reconstrucción depende de la cantidad de información biométrica recogida.

14. "La información biométrica no es interoperable"

Al contrario, los sistemas de tratamiento de información biométrica se desarrollan siguiendo estándares para garantizar su interoperabilidad[22].

Los sistemas que funcionan comparando el resultado de aplicar una función hash sobre los patrones biométricos también pueden hacerse interoperables por el sencillo método de compartir las claves utilizadas durante el proceso de hashing.

[21] En la página 3 se pueden comparar las caras originales y las caras reconstruidas a partir de los patrones:
https://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf

[22] Ejemplo de conversión entre formatos biométricos:
https://jomutech.com/convertfingerprintimagestoisooransifingerprinttemplateformats/
Descripción de estándares de interoperabilidad biométrica:
http://biometria611.blogspot.com/p/estandares.html