MIS DATOS MIS DERECHOS

LEY

¿Qué ocurre cuando tu selfie o tus huellas se convierten en tu identidad digital?

Biometría y datos personales

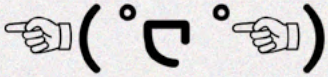
Biometría, ¿Qué es?

Son características físicas que permiten identificarnos de **forma única**.

Los datos biométricos describen las características fisiológicas y de comportamiento de los individuos. Son catalogados como **datos personales sensibles** y se dividen en dos grandes categorías.

- Por un lado, los que provienen de las características físicas y fisiológicas: las huellas dactilares, los rasgos faciales, geometría de la mano, marcha o perfiles de ADN, patrones de retina e iris, la forma de una parte del cuerpo como la mano o la oreja, e incluso el mapa de nuestras venas.
- Por otra parte, los que se refieren a ciertas características del comportamiento, como son la voz, la firma, el modo de andar o de escribir en un teclado.

Los gobiernos utilizan la biometría, por ejemplo, en los sistemas nacionales de identificación, para el registro de impuestos, así como el tránsito en zonas de fronteras. La biometría también se utiliza en iniciativas humanitarias y de desarrollo. En el sector privado la utilizan bancos o centros comerciales para el registro y control de sus clientes.



Procesamiento de la biometría

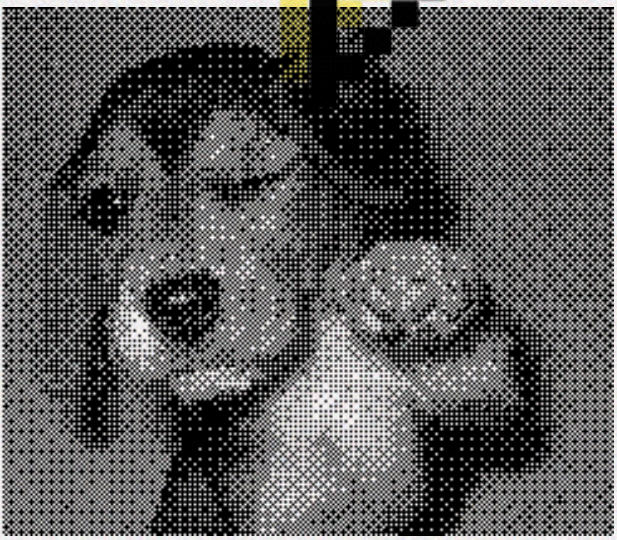
El empleo de cualquier **sistema biométrico** tiene dos partes.

- En primer lugar, las tecnologías biométricas capturan y almacenan características en una base de datos para identificar a un individuo.
- En segundo lugar, la información de esta base de datos “se cruza” para verificar o autentificar la identidad de un individuo en una serie de contextos, por ejemplo, al acceder a los servicios gubernamentales, o al atravesar fronteras, para permitir que un individuo vote, acceda a las cuentas bancarias, acceda a los servicios de salud, de impuestos, etc.

RIESGOS

- Los datos biométricos pueden identificar a una persona durante toda su vida. Permite individualizar y realizar un seguimiento preciso de cada persona.
- Uso encubierto o sin consentimiento de la población.
- Inversión de la carga de la prueba: todos son culpables hasta que el sistema/algoritmo determine que no lo son. Afectación a garantías del debido proceso.
- Discriminación: la tecnología es imprecisa y arroja un alto porcentaje de falsos positivos contra personas de tez no blanca y mujeres (además de otras comunidades en situación de vulnerabilidad). La precisión variable y los porcentajes de fallo de la tecnología pueden conducir a la identificación errónea, el fraude y la exclusión cívica.
- No existe una regulación detallada que establezca las garantías necesarias ni condiciones estrictas para su uso.
- Filtraciones o hackeos a la base de datos por una pobre o nula implementación de medidas de seguridad.
- Opacidad del sistema. A menudo no está claro cómo funcionan realmente los sistemas y, por lo tanto, por qué y cómo fallan, y cómo se reflexiona sobre las lecciones aprendidas. También hay una falta de claridad de los deberes y responsabilidades de las diferentes partes, especialmente cuando se están desplegando en un vacío legal y normativo.
- Facilita la vigilancia masiva en forma automatizada: los algoritmos de reconocimiento facial deben necesariamente detectar todos los rostros que registran las cámaras en donde están implementados. Por más que el nombre de una persona no esté vinculado a su rostro, el software igualmente lo estará reconociendo.

¿Qué debe hacer el Estado?



- Adoptar marcos jurídicos sólidos y salvaguardas estrictas (Ej: ley de protección de datos personales). Las tecnologías biométricas plantean graves amenazas para la privacidad y la seguridad personal, su aplicación puede facilitar y ampliar las discriminaciones y vigilancia masivas;
- Evaluar si las tecnologías biométricas resuelven realmente los problemas socio económicos que se pretenden resolver;
- Requerir a los Estados que la adquisición de la tecnología biométrica se base en justificaciones públicas y transparentes (motivación, costos y debate público);

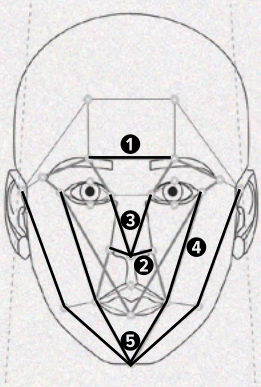
Tu selfie, tus datos

Reconocimiento facial y su funcionamiento

El reconocimiento facial no tiene que ver con tu cara, sino trata de cómo se puede utilizar tu identidad digital para determinar tus derechos.

Con cada selfie que te tomas y subís a Internet, creas un conjunto de datos sobre tus rasgos faciales: estos puntos nodales forman un conjunto único de características llamado huella facial, que puede utilizarse para identificarte sólo a vos y que está conformado por:

1. La distancia entre los ojos
2. La anchura de su nariz
3. la profundidad de las cuencas de los ojos
4. la forma de los pómulos
5. la longitud de la línea de la mandíbula



Las huellas faciales pueden convertirse en modelos 3D de tu cara que incluyen otras medidas, como la forma de las cuencas de los ojos o las curvas de la nariz y la mandíbula.

El reconocimiento facial puede hacer tu vida más eficiente al permitir a partir de tu rostro, abrir puertas, hacer transacciones, pagar servicios, obtener información puntual o acceder a mejores tratamientos, desbloquear tu teléfono o pagar algo con tu sonrisa. Esto parece relativamente inofensivo si pensás que tu cara sólo puede ser utilizada para confirmar tu identidad, y sólo cuando te importa.

¿Y si la misma huella facial puede utilizarse para mejorar las formas de vigilar tu comportamiento?

Por ejemplo: **¿a dónde vas? ¿cuándo? y ¿con quién?**

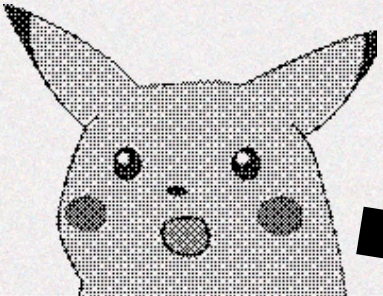
¿Y si puede determinar otras características sobre vos, como lo que piensas, tu estado de ánimo, tu coeficiente intelectual y sus orientaciones políticas o sexuales? Esa información puede utilizarse para ofrecerte información o contrainformación, rechazar o habilitar servicios, reasignar privilegios, ofrecer precios diferentes o determinar sus derechos.

¿Qué otros datos se pueden extraer de tu rostro?

- **Biometría de la piel:** como el reconocimiento facial, pero en lugar de una huella facial este método crea una huella cutánea a partir de la textura de de tu piel.
- **Escaneo del iris:** el reconocimiento del iris utiliza técnicas de reconocimiento de patrones matemáticos en el iris de tus ojos para identificarle biométricamente.
- **Escaneo de la retina:** utiliza los patrones únicos de los vasos sanguíneos de tu retina como identificación biométrica. Debido a su naturaleza única e inmutable, tu retina es probablemente el identificador biométrico más preciso y fiable, además de tu ADN.
- **Forma de la oreja:** el reconocimiento de la oreja basado en la extracción de características geométricas puede ser eficaz porque la forma de la oreja cambia muy poco con el tiempo

Los sistemas de reconocimiento facial pueden ser aún más eficaces para identificación cuando se combinan con otros métodos como:

- **Huellas dactilares y muestras de ADN:** los dos tipos más comunes de identificación biométrica
- **Reconocimiento del movimiento corporal:** analiza tus patrones de marcha desde distancia, observando todo tu cuerpo en movimiento
- **Reconocimiento de la voz:** te identifica basándose en las características de tu voz.
- **Reconocimiento de emociones:** identifica varios estados psicológicos a partir de tus rasgos faciales y/o tu voz.



El reconocimiento facial tiene
dos objetivos principales:

Objetivo 1

La identificación responde a la pregunta: **¿quién es esta persona?**

Se te puede identificar entre una multitud de otros rostros en tiempo real a través de fotografías, cámaras de CCTV o dispositivos de toma de imágenes que operan en otros espectros como el infrarrojo.

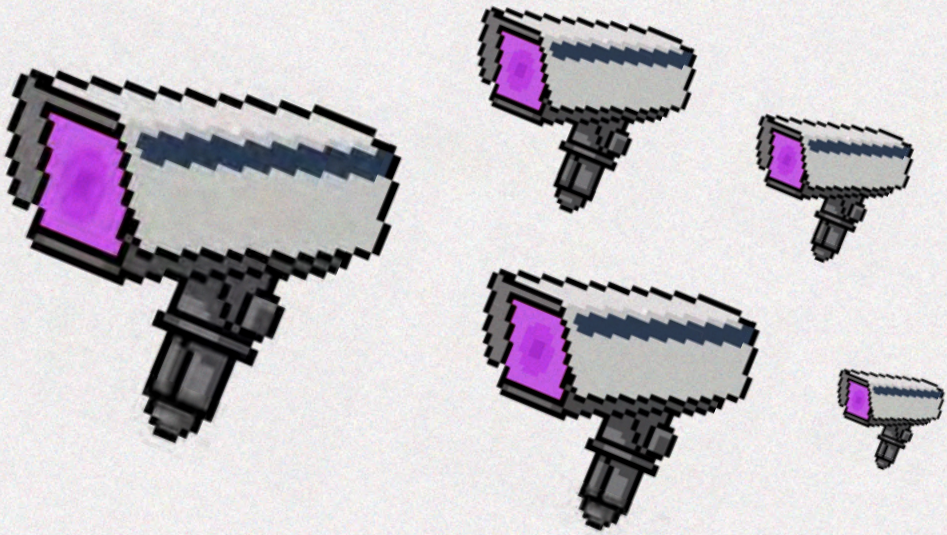
Objetivo 2

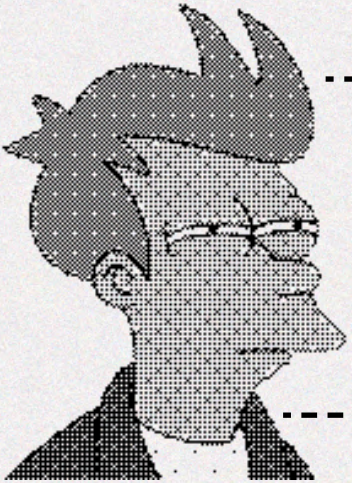
La verificación responde a la pregunta: **¿es esta persona quien dice ser?**

Este método compara tu rostro con otras fotografías o datos biométricos para confirmar tu identidad única.

Las huellas faciales pueden hacerse a partir de una selfie, pero también pueden crearse a partir de cualquier **fotografía o vídeo** que te hayan tomado, aunque no te hayas dado cuenta.

Por ejemplo, una huella facial puede generarse a partir de tu rostro en tiempo real mediante una **cámara de circuito cerrado de televisión (CCTV)**, o bien mediante tecnologías invisibles para el ojo humano, **como los infrarrojos o las imágenes térmicas**.





¿A quién le interesa tu selfie?

Los datos de tu rostro son buscados por las fuerzas del orden, los controles fronterizos, agencias de seguridad, agencias tributarias, la industria publicitaria, empresarios y agencias de espionaje, entre otros.

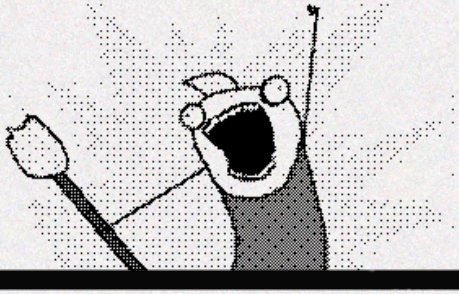
La escasa regulación de los datos biométricos hace que corran el riesgo de ser utilizados con fines no previstos, lo que viola los derechos de las personas al exponerlas a la elaboración de perfiles, la vigilancia y el control y la discriminación.

La identidad que no se puede cambiar

Estos datos únicos, generados a partir de las características de los seres humanos, pueden utilizarse para **rastrear y perfilar a las personas** a lo largo de su vida. El uso y el mal uso de estos datos tiene la trágica posibilidad de negar a una persona su identidad, sin posibilidad de recuperarla y sin la posibilidad de reparación del daño sufrido.

Tu huella facial, o una parte importante de ella, podría ser robada. O podrías recibir un correo electrónico con un vídeo que muestre tu cara haciendo cosas que vos que nunca has hecho o diciendo cosas que nunca has dicho. O alguien podría acceder a tus espacios personales utilizando tu iris. ¿Estarías cómoda si tu huella facial fuera accesible a cualquiera?

Por lo tanto, es esencial que la tecnología biométrica esté regulada y supervisada en todos los niveles de su uso empezando por su obtención, tratamiento y almacenamiento. Además, cada vez que se utilicen esos datos, debe garantizarse que sólo se utilizan para el fin previsto.



¿Qué debemos hacer?

Defiende tus derechos. El reconocimiento facial implementado en las calles de nuestras ciudades tiene un potencial de interferir directamente con derechos como la privacidad, libertad de expresión, de reunión, manifestación y asociación.

Sumate a la campaña y al debate público que buscan transparencia en la adquisición de tecnologías biométricas en tu país. ¿Para qué? ¿Dónde las quieren instalar? ¿Con qué base de datos se cruzará y analizará? ¿Quiénes tienen acceso? ¿Qué pasa si clonan nuestros datos biométricos? ¿Cuáles son las evaluaciones de riesgos? Entre otros.

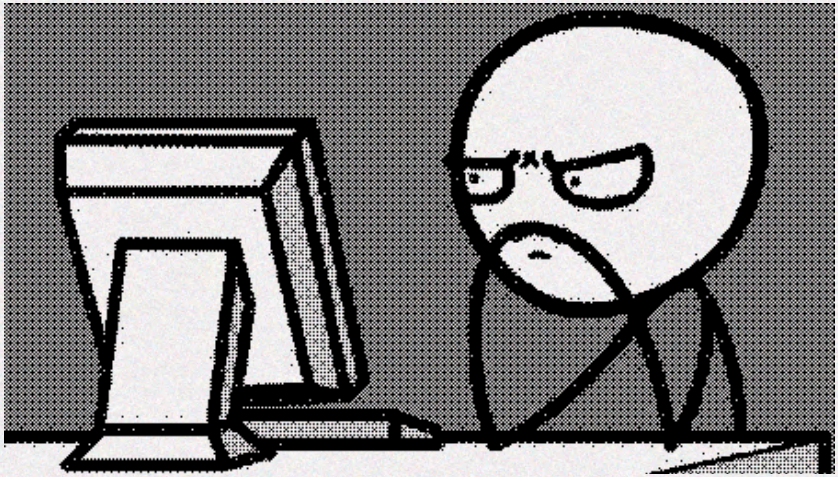
Evita utilizar esta tecnología si desconoces el marco legal donde se encuentran alojada tu información personal. Pregunta a la empresa (banco, shopping, co-working, estadio de fútbol) por sus políticas de privacidad para registrar tu rostro en sus sistemas. ¿Por cuánto tiempo lo almacenan? ¿Quiénes acceden a esos datos? ¿Por qué no utilizan otro mecanismo menos intrusivo a la privacidad para el registro de identidad? ¿Cuentan con permiso legal para el registro de tus datos biométricos sensibles?

Cubre tu rostro con máscaras cuando asistas a marchas o protestas para evitar el reconocimiento y exponerte riesgos como vigilancia, control, discriminación, elaboración de perfiles entre otros.

Obliga tu Estado a que cuente con marcos legales sólidos que garanticen la protección de tus datos para el acceso a los servicios en Internet.

Referencias

1. TEDIC (2018) – Investigación – La enajenación continua de nuestros derechos. Sistema de identidad: biometría y cámaras de vigilancia no reguladas en Paraguay. https://www.tedic.org/wp-content/uploads/2018/12/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018-2.pdf
2. TEDIC (2019) – Litigio estratégico - ¿Quién vigila al vigilante reconocimiento facial en Asunción?. https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/
3. Privacy International – Campaña - Aprende sobre biometría (inglés). https://privacyinternational.org/learn/biometrics
4. ADC – Campaña “Con mi cara no”. https://conmicarano.adc.org.ar/
5. R3D – Campaña “No nos vean la cara”. https://nonosveanlacara.r3d.mx/
6. Tactical Tech. Proyecto “The glass Room”. https://theglassroom.org



Esta fanzine fue realizada por la ONG TEDIC de Paraguay,
en el marco de la campaña de **Mis datos, mis derechos**.

TEDIC (Tecnología y Derechos Humanos) es una organización sin fines de lucro que defiende y promueve los derechos humanos en entornos digitales, con foco en desigualdades de género y sus intersecciones en Paraguay y la región de América Latina.

Licencia Creative Commons CC-BY-SA Versión 4.0 Internacional