NO_NOS VEAN_LA CARA

VIGILANCIA EN EL ESPACIO PÚBLICO CON TECNOLOGÍAS DE RECONOCIMIENTO FACIAL EN MÉXICO

R3D
Red en Defensa de los Derechos Digitales

Unión Europea

NO_NOS VEAN_LA CARA

R3D
Red en Defensa
de los Derechos Digitales

Unión
Europea

NO NOS VEAN LA CARA

VIGILANCIA EN EL ESPACIO PÚBLICO CON TECNOLOGÍAS DE RECONOCIMIENTO FACIAL EN MÉXICO

R3D: Red en Defensa de los Derechos Digitales
Escrito por: Francia Pietrasanta, Grecia Macías y Santiago Narváez
Editado por: José Flores
Portada e interiores: Gibrán Aquino

Mayo de 2025

R3D
Red en Defensa
de los Derechos Digitales

Unión
Europea

Este documento se ha realizado con la ayuda financiera de la Unión Europea. Su contenido es responsabilidad exclusiva de R3D y en modo alguno debe considerarse que refleja la posición de la Unión Europea.

Licencia de Creative Commons Reconocimiento-No-Comercial-CompartirIgual4.0 Internacional

ua

\ ÍNDICE

06 <Introducción></>

08 Cap01:\ RECONOCIMIENTO FACIAL 101. ¿CÓMO FUNCIONA LA TECNOLOGÍA DE RECONOCIMIENTO FACIAL Y CÓMO AFECTA A NUESTROS DERECHOS HUMANOS?

08 < ¿Qué es la tecnología de reconocimiento facial? />
08 */ *Inteligencia artificial*
09 */ *Sistemas de aprendizaje automático*
10 */ *Visión computacional*
10 */ *El ciclo de vida de la inteligencia artificial*
13 < Tecnología biométrica />
13 */ *¿Qué es un dato biométrico?*
13 */ *¿Cuáles son los principales procesos biométricos?*
15 */ *Tecnología de reconocimiento facial (TRF)*
16 */ *La tecnología de reconocimiento facial falla*
19 < La TRF pone en riesgo nuestros derechos humanos />
19 */ *Afectaciones al derecho a la privacidad*

32 Cap02:\ RECONOCIMIENTO FACIAL EN CIUDADES DE MÉXICO: LOS CASOS DE COAHUILA Y AGUASCALIENTES

32 < Sistema de Video Inteligencia para la Seguridad: el reconocimiento facial en Coahuila />
33 */ *Preocupaciones en torno al sistema de reconocimiento facial en Coahuila*
41 < Reconocimiento facial en Aguascalientes />
41 */ *Municipio de Aguascalientes: Videovigilancia Urbana Integral con Tecnología Analítica*
42 */ *Estado de Aguascalientes: C5 SITEC*
50 */ *Blindaje Aguascalientes: otras iniciativas estatales de reconocimiento facial*

52 Cap03:\ UNA SOLUCIÓN EN BÚSQUEDA DE UN PROBLEMA: LA IMPLEMENTACIÓN DE TRF EN AEROPUERTOS.

52 < La TRF en los aeropuertos del mundo />
53 < La TRF en el Aeropuerto Internacional Felipe Ángeles />
55 */ *Funcionamiento del Sistema de Procesamiento de Pasajeros del AIFA*
56 */ *Recolección y tratamiento de datos personales*
59 */ *Etapa de Enrolamiento*
60 */ *Etapa de Verificación*
60 */ *¿Qué tan confiable es el SPP?*

68 Cap04:\ RECONOCIMIENTO FACIAL EN ESTADIOS: NUESTROS DERECHOS EN JUEGO

69 < Reconocimiento facial en estadios: una mirada global />
73 < Fan ID en México: un sistema opaco e ineficiente />
75 */ *Obligatoriedad de la medida*
76 */ *Tratamiento de datos*
77 */ *Transferencias de datos a autoridades*
78 */ *La falta de efectividad del Fan ID*
80 < ¿Cómo afecta nuestros derechos la TRF en estadios? />
80 */ *Privacidad y protección de datos personales*
81 */ *Libertad de expresión y reunión pacífica*
82 */ *Igualdad y no discriminación*
83 */ *Acceso a la cultura*
84 */ *Presunción de inocencia*
85 < Necesidad de alternativas />
87 < Contra la normalización de la TRF en los estadios />

90 <Conclusiones> No nos vean la cara </Conclusiones>

INTRODUCCIÓN

Las personas tienen derecho a apropiarse del espacio público. En la calle, parques, estadios, museos y otros lugares definimos nuestra personalidad y creamos comunidad. Para que las personas puedan apropiarse de estos espacios, es necesario que puedan desenvolverse libremente sin injerencias arbitrarias de terceros.

Hoy en día, los espacios públicos son un campo de batalla. Las tecnologías con capacidad de reconocimiento facial (en adelante, TRF) han sido promocionadas como la solución de todos los problemas de seguridad, particularmente en América Latina. Distintos gobiernos han buscado limitar las libertades en estos ámbitos para controlar a la población. La narrativa de la securitización de lo público ha sido utilizada para justificar políticas autoritarias como la implementación de tecnologías de vigilancia masiva.

Poder identificar a una persona con su rostro, de manera remota y sin su consentimiento, supone que no podemos a salir a la calle de manera anónima. Quien nos observe en el espacio público puede ir encontrando patrones que desglosen quiénes somos, cuáles son nuestras afinidades pollíticas, religiosas, orientación sexual y cualquier aspecto relacionado con nuestra personalidad.

Durante años, desde Red en Defensa de los Derechos Digitales hemos documentado la implementación de TRF en México. En este reporte nos centramos en tres principales formas en las que se han desplegado estas tecnologías: en ciudades, en aeropuertos y en estadios.

En este informe nos dedicamos a desmitificar estas tecnologías y exponer la forma en la que las TRF afectan a los derechos humanos. En el primer apartado, hacemos un recuento de su funcionamiento y explicamos los conceptos esenciales para poder entender estas tecnologías, como los datos que recogen, su funcionamiento y qué derechos se ven afectados por su uso.

En el segundo apartado, exponemos el uso de TRF en ciudades, a través de la documentación de casos en los estados de Coahuila y Aguascalientes. En este apartado problematizamos la falta de legislación, transparencia y rendición de cuentas que existe alrededor del uso de estas tecnologías.

En el tercer apartado abordamos el caso de los aeropuertos y las TRF. A lo largo de los últimos dos años, hemos documentado su uso en el Aeropuerto Internacional Felipe Ángeles (AIFA). Problematizamos la supuesta necesidad de usar sistemas de identificación biométrica en los aeropuertos para agilizar servicios y brindar seguridad a las personas. Igualmente, hacemos un recuento de la opacidad alrededor de la implementación de estos sistemas y las problemáticas que surgen derivadas de esta falta de transparencia.

Finalmente, en el cuarto apartado evaluamos el reconocimiento facial en estadios como una solución a los problemas de seguridad y violencia. Explicamos cómo la TRF sacrifica los derechos humanos de las personas en los estadios y analizamos la implementación de esta tecnología a nivel mundial, con énfasis en el caso del Fan ID en México. Además, proponemos un enfoque que puede ser útil para la búsqueda de soluciones menos invasivas para los derechos humanos.

Este informe es producto de más de cuatro años de investigación y litigios de transparencia. Las TRF se propagan con rapidez, sin que exista un ejercicio crítico detrás de su implementación. Los casos que exponemos a continuación son ilustrativos de que las tecnologías de reconocimiento facial en espacios públicos suponen graves riesgos a los derechos humanos y a las democracias en general.

Esperamos que este informe sirva como una herramienta que desmienta todas las promesas falsas del tecnosolucionismo y ponga en duda la convicción de que la TRF garantiza seguridad.

CAP.01\\

RECONOCIMIENTO FACIAL 101. ¿CÓMO FUNCIONA LA TECNOLOGÍA DE RECONOCIMIENTO FACIAL Y CÓMO AFECTA A NUESTROS DERECHOS HUMANOS?

En la última década, la tecnología de reconocimiento facial se ha incrustado en el inconsciente colectivo como una solución mágica para los problemas de seguridad pública. Esta narrativa, alimentada por la idea de que los algoritmos son capaces de realizar tareas sobrehumanas y milagrosas, ha promovido la adopción irreflexiva de herramientas de vigilancia biométrica por parte de autoridades y empresas.

Por el contrario, estas herramientas están lejos de ser perfectas: recolectan información de manera masiva e indiscriminada, tienen tasas de error considerables y reproducen sesgos que amplifican las brechas de discriminación y exclusión social.

La opacidad con la que operan las tecnologías de reconocimiento facial han llevado a que sus promotores pidan a la sociedad que dé un salto de fe, sin cuestionar su funcionamiento ni las consecuencias que generan, en especial en poblaciones en situación de vulnerabilidad. Por tanto, resulta indispensable que la sociedad comprenda cómo funcionan estos sistemas para poder confrontar y resistir estas narrativas tecnosolucionistas.

En este primer apartado, nos centraremos en explicar los conceptos básicos relacionados con el funcionamiento de las TRF. Posteriormente, haremos un recuento del ciclo de vida para entender de mejor manera los efectos que tiene esta tecnología en los derechos de las personas.

¿QUÉ ES LA TECNOLOGÍA DE RECONOCIMIENTO FACIAL?

La tecnología de reconocimiento facial es, en su definición más simple, un sistema que analiza las características del rostro para identificar o verificar la identidad de una persona.

Sin embargo, para entender con mayor profundidad cómo funciona la TRF, es importante aclarar tres conceptos: 1) la inteligencia artificial, 2) los sistemas de aprendizaje automatizado y 3) la tecnología biométrica.

INTELIGENCIA ARTIFICIAL

El concepto de *inteligencia artificial* existe desde hace más de sesenta años. No obstante, en los últimos años, este término parece ubicuo en las tecnologías digitales. Aunque no hay una definición única de inteligencia artificial, la OCDE lo define como:

> Sistemas que pueden realizar tareas o hacer predicciones, recomendaciones o decisiones que usualmente requieren inteligencia humana. Los sistemas de IA pueden realizar estas tareas y tomar decisiones basadas en los objetivos que establecieron las personas pero sin instrucciones humanas explícitas.[1]

La *inteligencia artificial* funciona como un término paraguas que abarca muchos tipos de sistemas automatizados, no solamente los modelos de lenguaje de gran tamaño (LLM, por sus siglas en inglés) o los sistemas generativos.

Por su amplitud, la conceptualización de la inteligencia artificial (IA) es sumamente controvertida. Académicos y activistas han criticado este concepto por crear una caja negra alrededor de tecnologías –como el reconocimiento facial– que afectan a toda la población.

Existen diversos modelos categorizados dentro de la etiqueta de *inteligencia artificial*. En el caso de la tecnología con capacidades de reconocimiento facial, se reconocen dos grandes ramas de la programación: el aprendizaje automático (*machine learning*) y la visión computacional (*computer vision*):

SISTEMAS DE APRENDIZAJE AUTOMÁTICO

Los sistemas de aprendizaje automático (ML, *machine learning*) han predominado en el ámbito del desarrollo tecnológico. Aunque existen distintos tipos, el más común es el que clasifica información.

La tecnología de ML es un sistema computacional del cual se espera que aprenda de la experiencia de entrenar con una serie de clases de tareas y una medida de desempeño".[2] En otras palabras, entre más entrene con una clasificación correcta, va a adquirir más experiencia y podrá replicarlo de mejor manera en futuras ocasiones.[3]

Un sistema de aprendizaje automático extrae patrones de una colección de datos que le sirvan para realizar una tarea en específico. Estos patrones se identifican por un "aprendizaje" que realiza el código previamente.[4] El objetivo principal de ML es poder hacer predicciones o generalizaciones acertadas con la información nueva que se le presente, usando como base los datos de entrenamiento con los que aprendió a hacer dichas predicciones.[5] Estos sistemas están programados con dos grandes pasos en el procedimiento de aprendizaje: el paso de entrenamiento y el paso de evaluación.

//* ----------

01/ Organización para la Cooperación y el Desarrollo Económico. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Publicado el 21 de mayo de 2019.

02/ Tom M. Mitchell, *Machine Learning*, McGraw-Hill Series in Computer Science (New York: McGraw-Hill, 1997). P. 2-5

03/ *Idem*.

04/ Patrick Nutter, "Machine Learning Evidence: Admissibility and Weight", *University of Pennsylvania Journal of Constitutional Law* 21, núm. 3 (el 1 de febrero de 2019): 929, https://scholarship.law.upenn.edu/jcl/vol21/iss3/8

El entrenamiento de algoritmos se realiza con una base de datos de entrenamiento y las clasificaciones asignadas a esos datos por la persona programadora.[6] En un segundo momento, el sistema automatizado se evalúa con una base de datos de referencia y realiza asociaciones al enfrentarse a nueva información conforme a los casos y pruebas que ha realizado con los datos de entrenamiento.

El aprendizaje de sistemas de ML puede ser supervisado, no supervisado o semi supervisado.[7] El aprendizaje supervisado sucede en los sistemas donde todos los datos de entrenamiento están etiquetados, usualmente por un ser humano, con una clasificación determinada.[8]

El aprendizaje no supervisado ocurre cuando los datos recolectados no están etiquetados y el mismo sistema trata de encontrar patrones o consistencias en los datos de entrenamiento e infiere las etiquetas.[9] El tercer tipo de aprendizaje es el semi supervisado, donde alguno de los datos sí están etiquetados y otros no.[10]

VISIÓN COMPUTACIONAL

La visión computacional (también conocida como *computer vision*) es la tecnología por la cual las computadoras traducen una imagen al lenguaje de programación. El fin último de la investigación sobre visión computacional es proveer a las computadoras de percibir el entorno como lo hacemos los seres humanos, entender los datos percibidos, tomar acción y aprender de esa experiencia para futuras ocasiones.[11]

La tecnología de visión computacional ha tenido avances significativos en los últimos años pero hasta ahora no se ha podido replicar la visión humana a la perfección.[12] No obstante, ha sido implementada para usos como reconocer tipos de peces, conducción de automóviles en piloto automático y sistemas de vigilancia biométrica.

EL CICLO DE VIDA DE LA INTELIGENCIA ARTIFICIAL

En general, todos los procesos algorítmicos tienen un "ciclo de vida". Normalmente se dividen en la investigación, la concepción y el desarrollo hasta el despliegue y la utilización, pasando

//* ----------

05/ Pedro Domingos, "A Few Useful Things to Know about Machine Learning", *Communications of the ACM 55*, núm. 10 (octubre de 2012): 78–87, https://doi.org/10.1145/2347736.2347755

06/ Esto aplica en el caso de aprendizaje supervisado y en algunos casos del aprendizaje semi supervisado.

07/ Nicu Sebe, ed., *Machine learning in computer vision*, Computational imaging and vision, v. 29 (Dordrecht: Springer, 2005). P.7

08/ *Idem.*

09/ *Id.*

10/ *Id.*

11/ Id. Sebe, *Machine learning in computer vision*, 1–2. P. 1-2

12/ *Machine learning for computer vision*, Studies in computational intelligence 411 (Berlin: Springer, 2013).

por el mantenimiento, el funcionamiento, la comercialización, la financiación, el seguimiento y la evaluación, la validación, el fin de la utilización, el desmontaje y la terminación.[13]

Es importante distinguir cada una de las etapas o fases para poder dilucidar las tareas que se llevan a cabo, las obligaciones que deben cumplirse y conocer qué tipo de errores pueden actualizarse. El ciclo de vida de la TRF tiene distintas fases, donde se realizan distintas tareas y también pueden actualizarse errores en específico.

01// **Recolección de datos de entrenamiento:** la recolección, etiquetado, clasificación y curación de las bases de datos de imágenes faciales que los desarrolladores usan para entrenar los algoritmos para poder identificar los marcos faciales.[14]

02// **Desarrollo del algoritmo:** la fase donde se programa y entrena al algoritmo. Se crea una red neuronal y se le entrena con muchas cantidades de imágenes para reducir la tasa de error del algoritmo. Aquí es donde se hacen la mayoría de las pruebas para poder analizar si está realizando bien las identificaciones de rostros, el porcentaje de certeza en las identificaciones y donde se debe hacer transparencia para conocer el rango de error.

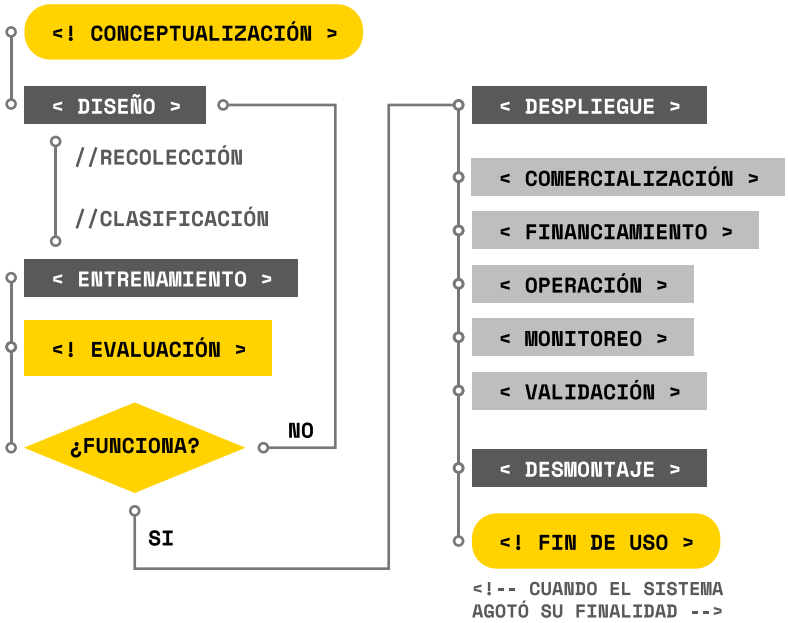
03// **Integración de software:** es la etapa donde se convierte el modelo computacional en aplicaciones más accesibles para los clientes. Así mismo, en esta fase se venden los sistemas terminados a los operadores.[15]

//* ----------

13/ UNESCO. "Recomendación sobre la ética de la inteligencia artificial". SHS/BIO/PI/2021/1. 23 de noviembre de 2021.

14/ Amy K. Lehr y William Crumpler, "Facing the Risk Part 1: Mapping the Human Rights Risks in the Development of Facial Recognition Technology" (CSIS Strategic Technologies Program and the Human Rights Initiative, el 27 de julio de 2021). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210727_Lehr_FacingtheRisk_One_1.pdf?iT5sia0du2_S.L4E1jr63ThOOexlTipk

15/ *Id.*



La etapa de despliegue es el momento de implementación del sistema de TRF, es decir, cuando el sistema se empieza a utilizar fuera de un contexto controlado y con situaciones del día a día. La comercialización es todo el proceso de promoción y venta del producto a pequeña o gran escala. La etapa de financiamiento ocurre cuando se encuentra a un cliente que compra tanto el producto como su instalación.

Una vez instalado, el cliente puede operar por sí mismo el algoritmo o pedir que el desarrollador de la TRF sea quien lo maneje. Las últimas etapas de monitoreo y validación son constantes, pues tanto las empresas responsables de desarrollar la TRF como los clientes deben de hacer una documentación de cómo se está utilizando la tecnología y validar que se estén siguiendo los estándares de calidad. Finalmente, cuando el sistema agote su uso, el cliente y la empresa desarrolladora deberán de desmontar su instalación, eliminar los datos de manera segura y ponerle fin a su uso.

TECNOLOGÍA BIOMÉTRICA

¿QUÉ ES UN DATO BIOMÉTRICO?

Los datos biométricos son datos personales relacionados a las características físicas, fisiológicas o conductuales de una persona física que, a través de un procesamiento tecnológico en específico, permiten o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.[16] Esto incluye la voz, el iris de los ojos, la huella digital, rasgos faciales, entre otros.

Los sistemas biométricos, por el otro lado, se refieren a los métodos automáticos que, con base en determinadas características humanas, identifican y autentifican a las personas.[17]

¿CUÁLES SON LOS PRINCIPALES PROCESOS BIOMÉTRICOS?

Los procesos biométricos se clasifican de acuerdo a los siguientes objetivos:[18]

01// Probar que una persona es quien dice ser.

02// Probar que una persona no es quien dice no ser.

Para lograr estos objetivos se usan las técnicas de identificación y autenticación (también conocida como verificación). El proceso de identificación consiste en "determinar la identidad de una persona cuando no se conoce, es decir, responder a la pregunta ¿quién es ella?"[19] La identificación usualmente se describe como un proceso de concordancia (1:N), pues la presentación de una plantilla biométrica es creada en tiempo real –también conocida como un *biométrico en vivo*– y se contrasta con una base de datos de plantillas biométricas.

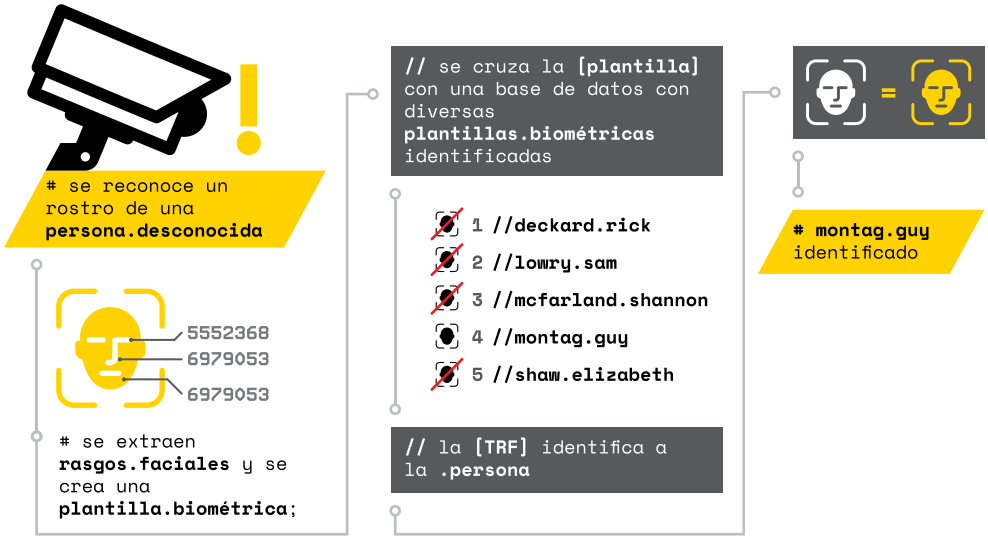
//* ----------

16/ Reglamento(UE) 2016/679 del Parlamento Europeo y Del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento Europeo)

17/ Leandro Ucciferri, "Tu yo digital. Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México" (Argentina: Asociación por los Derechos Civiles, abril de 2019), 7–8, https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf

18/ William Abernathy y Lee Tien, "Biometrics: Who 's Watching You?" (Electronic Frontier Foundation, el 14 de septiembre de 2003), https://www.eff.org/es/wp/biometrics-whos-watching-you

19/ Shoshana Magnet, When biometrics fail: gender, race, and the technology of identity (Durham: Duke University Press, 2011), 21.

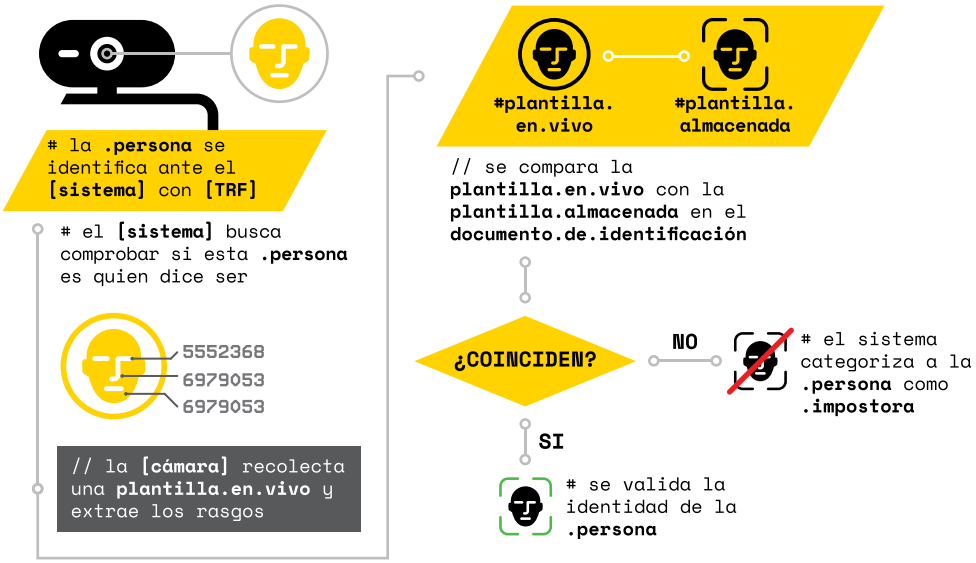


Por el otro lado, la autenticación consiste en verificar la identidad que una persona ostenta, es decir, se hace la pregunta: ¿es ella la persona que dice ser?[20] Esto también se conoce como un proceso de concordancia 1:1. La autenticación revisa la representación del biométrico en vivo (por ejemplo, una persona frente a la cámara), con la única plantilla de la persona almacenada en el sistema o en un soporte material para ver si coinciden. Si el sistema de verificación determina que el biométrico en vivo es el mismo que la plantilla biométrica guardada, hay concordancia y se verifica la identidad.[21]

//* ----------

20/ *Idem.*

21/ *Idem.*



TECNOLOGÍA DE RECONOCIMIENTO FACIAL (TRF)

La tecnología de procesamiento o reconocimiento facial incluye distintos procesos algorítmicos: detección facial, análisis facial y la identificación o verificación del marco facial con una persona.[22]

La detección facial ocurre cuando el sistema ubica un rostro dentro de una imagen. Primero, el sistema tiene que reconocer en las fotos o videos en vivo el área donde se encuentra un rostro. Después, el sistema tiene que hacer la normalización geométrica y de iluminación del rostro; se *recorta* el rostro capturado, se ajusta a un marco estándar y se hace correción de color.[23]

El análisis facial determina las características faciales de una persona a partir del dato biométrico del rostro y a partir de los rasgos físicos o demográficos de las personas.[24] Las imágenes digitales de los rostros se reducen a partes componentes identificables y se crea un marco facial digital.[25] El marco facial digital es como una huella digital, un mapa escrito en código que mide la distancia entre los rasgos, líneas o elementos faciales, entre otros.[26]

//* ----------

22/ Inioluwa Deborah Raji et al., "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing", en *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (AIES '20: AAAI/ACM Conference on AI, Ethics, and Society, New York NY USA: ACM, 2020), 7–8, https://doi.org/10.1145/3375627.3375820

23/ S. Z. Li y Anil K. Jain, eds., *Handbook of face recognition*, 2nd ed (London : New York: Springer, 2011), 4.

24/ Id. Inioluwa Deborah Raji et al. "Saving Face..."op. cit.16

25/ In the Face of Danger. Facial Recognition and the Limits of Privacy Law, 120 HARV. L. REV. 1870, 1870-71 (2007).

26/ Kirill Levashov, The Rise of A New Type of Surveillance for Which the Law Wasn't Ready, 15 COLUM. SCI. & TECH. L. REV. 164, 167 (2013).

Finalmente, para lograr la identificación o verificación biométrica, se realiza la comparación entre el rostro en vivo y el único o varios marcos del rostro contenidos en una base de datos.

Los rasgos extraídos por el algoritmo y establecer una métrica adecuada para confirmar la identidad de las personas son de los puntos más importantes para determinar el grado de precisión de una TRF. El sistema no señala de manera categórica la identidad de una persona, más bien hace un estimado porcentual de las similitudes entre los rostros comparados.[27]

En procesos de identificación biométrica (1:N) con reconocimiento facial, el sistema arroja la identidad de la persona cuando tiene el porcentaje de confianza suficiente para indicar que existe coincidencia entre el rostro en vivo y el marco facial identificado. En caso de que el porcentaje de coincidencia sea menor al indicador establecido, se considerará que no se ha identificado a la persona.[28]

Los procesos de verificación biométrica 1:1, el sistema simplemente dice si el rostro en vivo corresponde al único rostro almacenado en el sistema. En caso de que corresponda, la respuesta será afirmativa; en el caso contrario, la respuesta del sistema será negativa.

LA TECNOLOGÍA DE RECONOCIMIENTO FACIAL FALLA

La TRF falla por distintas razones: cámaras mal instaladas, bases de datos sesgadas, algoritmos imprecisos. Existen tres categorías de errores que se presentan en la operación de estos sistemas de identificación biométrica con personas:

- **Fallas para ingresar al sistema.** Existen casos en que las personas no pueden siquiera ingresar sus datos biométricos a la base de datos.[29] Esto puede ocurrir por diversos motivos. Por ejemplo, las huellas dactilares suelen desaparecer con la edad, por lo que las personas adultas mayores encuentran obstáculos al momento de registrar sus datos. De igual forma, las personas con discapacidad se ven especialmente afectadas para poder ingresas sus datos en sistemas biométricos, particulamente en TRF. Estos sistemas se basan sobre un concepto capacitista[30] sobre cómo debe verse el cuerpo humano, por lo cual no consideran la diversidad personas que se apartan de ese modelo único de cuerpo.
- **Tasa de falsa aceptación o falso positivo.** Este tipo de error ocurre cuando el sistema determina de manera incorrecta que una persona es quien el sistema intenta identificar. Este es el error mediante el cual puede ocurrir la detención de personas inocentes, las cuales son identificadas erróneamente por el sistema como la perso-

//* ----------

27/ Li,Stan Z., Jain, Anil K., et. al. “Handbook of Face Recognition”.

28/ Id. Li,Stan Z., Jain, Anil K., et. al. “Handbook of Face Recognition”(...).

29/ Amielle Magnet, Shoshana. “Chapter 1: Biometric Failure. When Biometrics Fail” Duke University Press p. 21.

30/ Tiffany Lee, “Biometrics and Disability Rights: Legal Compliance in Biometric Identification Programs,” University of Illinois Journal of Law, Technology & Policy 2016, no. 2 (Fall 2016): 209-244

na sospechosa o culpable, como ha ocurrido en sistemas de reconocimiento facial utilizados en Argentina,[31] Brasil,[32] Estados Unidos,[33] entre otros.

- **Tasa de falso rechazo o negativo.** Este tipo de error ocurre cuando la TRF el sistema ocurre cuando el sistema rechaza la identificación de un perfil porque no concuerdan a pesar de que sí es la misma persona. Un ejemplo de este error podría ocurrir cuando una persona quiere acceder a un sevicio pero el sistema la rechaza diciendo que no es quien dice ser.

Los principales factores que generan que las TRF fallen pueden dividirse en aquellos que están relacionados directamente con el proceso algorítmico y los factores ajenos al proceso algorítmico pero que aún así afectan su certeza.

A. Factores relacionados con el proceso algorítmico

Bases de datos poco diversas. Es necesaria un cantidad masiva de información para entrenar y evaluar correctamente a estos sistemas. Esto en sí mismo supone un grave riesgo a la privacidad, así como es improbable que una base de datos logre captar de manera adecuada la diversidad de rostros humanos sin ningún tipo de sesgo.[34] La composición de ciertas características, como la raza o el género en las bases de datos, influyen en la certeza del mismo. Por ejemplo, una subrepresentación de un grupo racial produce que el algoritmo tenga una tasa de error más alta para dicho conjunto.[35]

Un estudio sobre 189 algoritmos realizado por el Instituto Nacional de Tecnología y Estándares (NIST) del gobierno de Estados Unidos encontró tasas de error más altas al identificar personas con rasgos no caucásicos.[36] Igualmente, el Instituto de Tecnología de Massachu-

//* ----------

31/ Seis días arrestado por un error del sistema de reconocimiento facial. Página 12. Consulta en: https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

32/ Antônio Werneck. Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa. O GOBO. Consulta en: https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913?versao=amp

33/ Hill Kashmir. Wrongfully Accused by an Algorithm. New York Times. Consulta en: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html#click=https://t.co/KxKC81AEFV

34/ Learned-Miller, et al., "Facial Recognition Technologies in the Wild: A Call for a Federal Office and the Supplemental Document Facial Recognition Technologies: A Primer", 45–46.

35/ Erik Learned-Miller, et al., "Facial Recognition Technologies in the Wild: A Call for a Federal Office and the Supplemental Document Facial Recognition Technologies: A Primer" (Algorithmic Justice League, el 29 de abril de 2020), 9, https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf

36/ Patrick Grother, Mei Ngan, y Kayee Hanaoka, "Face Recognition Vendor Test Part 3:: Demographic Effects" (Gaithersburg, MD: National Institute of Standards and Technology, diciembre de 2019), https://doi.org/10.6028/NIST.IR.8280

setts (MIT) descubrió en que la tasa de error en los algoritmos más utilizados por TRF era entre 12 y 19 por ciento más alta en el proceso de reconocimiento de personas con tonos de piel más oscuros.[37]

Fallas en la etapa de evaluación. Una vez que el sistema es entrenado, se somete a evaluación con alguna base de datos de referencia. Esta evaluación se realiza con ciertos indicadores que sirven para identificar si el algoritmo está cumpliendo con el objetivo de identificar rostros de manera adecuada. Si bien los indicadores y los datos de referencia pueden describir el desempeño de TRF en ciertos casos controlados, no garantizan que estos sistemas puedan lograr con éxito cumplir sus funciones bajo nuevos escenarios que no fueron evaluados.[38]

La organización Algorithmic Justice League destaca el sobreajuste (*overfit*)[39] como un factor que incrementa las tasas de error en las TRF. El sobreajuste ocurre cuando una base de datos logra cumplir su objetivo con los datos de entrenamiento pero no puede replicar su efectividad en la fase de implementación con bases de datos distintas.

Esto ocurre porque las empresas que desarrollan TRF buscan cumplir con las evaluaciones para ser mejor calificados y usan los mismos indicadores y datos de referencia en exceso.[40] En este sentido, las TRF se desarrollan, incluso de manera involuntaria, para cumplir con las "preguntas" de las evaluaciones pero su precisión disminuye al enfrentarse a escenarios no controlados del día a día.

No existe evidencia irrefutable sobre alguna TRF que sea totalmente precisa. Las métricas se usan para medir el desempeño de una TRF respecto a un indicador (tasa de error, porcentaje de falsos negativos, falsos positivos, etc). No obstante, estas métricas no son universales, depende los datos de referencia e indicadores en específico que se estén usando y de la interpretación de la persona que está evaluando.[41]

Por ejemplo, un reporte del NIST[42] evaluó que, cuando algunos sistemas usaban dos fotos al azar de individuos distintos, tenían una tasa de error de falso positivo baja; es decir, el algoritmo casi no confundía a dos personas distintas con una sola persona. Por el contrario,

//* ----------

37/ Buolamwini Joy, Gebru Timnit. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" Proceedings of Machine Learning Research 81:1–15, 2018 Consulta en: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

38/ Cfr. Learned-Miller, et al., "Facial Recognition Technologies in the Wild: A Call for a Federal Office and the Supplemental Document Facial Recognition Technologies: A Primer", 4.

39/ Ver. Daniel Bashir et al., "An Information-Theoretic Perspective on Overfitting and Underfitting", en *AI 2020: Advances in Artificial Intelligence*, ed. Marcus Gallagher, Nour Moustafa, y Erandi Lakshika, vol. 12576, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2020), 1–6, https://doi.org/10.1007/978-3-030-64984-5_27

40/ Id. 43-44

41/ Learned-Miller, et al., "Facial Recognition Technologies in the Wild: A Call for a Federal Office and the Supplemental Document Facial Recognition Technologies: A Primer", 44.

42/ Patrick J. Grother, Mei L. Ngan, y Kayee K. Hanaoka, "Face Recognition Vendor Test Part 3: Demographic Effects", *NIST*, el 19 de diciembre de 2019, 2–5, https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects. Citado en: Learned-Miller, et al., "Facial Recognition Technologies in the Wild: A Call for a Federal Office and the Supplemental Document Facial Recognition Technologies: A Primer", 44–45.

cuando las imágenes comparadas eran de personas del mismo género, país o edad, el error de falso positivo ocurría 30 veces más a comparación de la evaluación anterior.

B. Factores exógenos al proceso algorítmico

Condiciones como la iluminación, la resolución de las imágenes, el ángulo del rostro, la exposición de este, tanto en las imágenes de la base de datos como en las imágenes en vivo, son factores que afectan el rendimiento de los sistemas de reconocimiento facial.

+ LA TRF PONE EN RIESGO NUESTROS DERECHOS HUMANOS

AFECTACIONES AL DERECHO A LA PRIVACIDAD

Las TRF afectan principalmente el derecho a la privacidad por el tratamiento masivo de datos biométricos. En 2022, la Suprema Corte de Justicia de la Unión (en adelante SCJN) resolvió que la recopilación y tratamiento masivo de datos biométricos que incluya a cualquier persona y que estas bases sean usadas o transferidas al Estado —especialmente cuando se trate de una retención permanente y sin una temporalidad específica—representa una afectación intensa a los derechos a la privacidad y protección de datos.[43]

El Parlamento Europeo ha definido que los datos biométricos se encuentran en una categoría especial de protección de datos personales pues "son tratados con medios técnicos específicos que permite la identificación o la autenticación unívoca de una persona física".[44] En este sentido, solo se pueden usar datos biométricos cuando haya consentimiento explícito para el tratamiento de los datos personales y sea necesario por razones de un interés público.[45]

Como explicamos anteriormente, el reconocimiento facial convierte las imágenes digitales de los rostros y los reduce a partes componentes identificables.[46] El marco facial digital es como una huella digital, un mapa escrito en código que mide la distancia entre los rasgos, líneas o elementos faciales, entre otros.[47] Al ubicarse en el espacio público, recolectando imágenes de cualquier persona que pase frente a ellas, las cámaras están recabando información de una esfera íntima de las personas.

Las personas, en general, esperamos en cierto grado privacidad cuando salimos a la calle.

//* ----------

43/ Pleno de la Suprema Corte de Justicia de la Nación. Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021, páginas 91 y 94.

44/ Reglamento (UE). Par. 51

45/ *Id.* artículo 9 apartado 1 y 2 inciso a y g.

46/ In the Face of Danger: Facial Recognition and the Limits of Privacy Law, 120 HARV. L. REV. 1870, 1870-71 (2007).

47/ Véase: Kirill Levashov, The Rise of A New Type of Surveillance for Which the Law Wasn't Ready, 15 COLUM. SCI. & TECH. L. REV. 164, 167 (2013).

Por ejemplo, no pensamos que alguien está siguiendo cada uno de nuestros movimientos cuando visitamos a alguien o acudimos al supermercado. Nuestras actividades en público cambiarían radicalmente si tuvieramos la sospecha de estar bajo constante vigilancia.

El concepto de expectativa de privacidad se ha reconocido por la Suprema Corte de Justicia de Estados Unidos[48] así como por el Tribunal Europeo de Derechos Humanos (en adelante, TEDH). Este concepto se refiere hasta qué grado las personas pueden esperar tener privacidad en espacios públicos sin ser sujetos a vigilancia como uno de los factores para decidir si existió una violación al derecho a la privacidad.

No todo lo que se manifiesta en el ámbito público implica una pérdida del derecho a la privacidad. El espacio público tiene dos dimensiones: una material y una política. La primera refiere al espacio, infraestructura, elementos físicos, etcétera, de un lugar que es público (un parque, las calles); la segunda corresponde a la acción humana, el nivel simbólico y el espacio de participación donde las personas se encuentran como agentes morales con derechos, intereses y una voz para expresarlos. En la dimensión política entran en juego las prácticas, los usos y los hábitos de las personas y los grupos de una sociedad, así como las normas sociales que existen entre ellos.[49]

Asimismo, el Comité de Derechos Humanos se ha pronunciado sobre la privacidad en el espacio público. En la Observación General No.37 establecen que "el simple hecho que los participantes en las asambleas estén en público no significa que su privacidad pueda ser restringida".[50] De igual forma, el TEDH ha señalado en distintos casos[51] que la vigilancia por video constituyó una intrusión a la vida privada donde no se cumplía con el margen de expectativa de privacidad.

La tecnología de reconocimiento facial involucra el procesamiento de mapas biométricos e imágenes faciales obtenidas en un espacio público con el propósito de determinar la identidad de una persona.[52] Al realizar esta operación de manera prolongada en el tiempo, el sistema adquiere y registra otros datos de su vida diaria como su rutina, las personas que se relacionan con ella u otros elementos relevantes de su personalidad y vida íntima. Igualmente, la vigilancia con herramientas de reconocimiento facial sirve a políticas de perfilamiento: categorizar individuos con base en sus características observables, como el origen racial o étnico.[53]

//* ----------

48/ Suprema Corte de Justicia de Estados Unidos. *United States vs Jones.* 615 F. 3d 544 (2012)

49/ R3D: Red en Defensa de los Derechos Digitales. "Videovigilancia en el espacio público: un obstáculo para las libertades civiles" enero 2020. Consulta en: https://r3d.mx/2020/01/29/videovigilancia-en-el-espacio-publico-un-obstaculo-para-las-libertades-civiles/

50/ Comité de Derechos Humanos. Observación General no. 37. Artículo 21: derecho a la reunión pacífica. 27 de julio de 2020, C/20/27, párr. 60-63

51/ Antović and Mirković v. Montenegro y Lopez Ribalda y otros contra España.

52/ European Agency For Fundamental Rights. " Facial recognition technology: fundamental rights considerations in law enforcement" Noviembre 2019. Consulta en: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

53/ European Agency For Fundamental Rights. "Preventing unlawful profiling today and in the future: a guide" p. 15 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

En el sistema interamericano, la Corte IDH también reconoce que un rasgo esencial de la privacidad es que es un espacio que "se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad".[54] La Corte IDH reconoce que el desarrollo de las tecnologías y la fluidez informativa colocal el derecho a la privacidad en una situación de mayor riesgo, por lo cual los estados deben asumir mayores responsabilidades para proteger efectivamente el derecho a al vida privada.[55]

La legislación mexicana en materia de protección de datos personales considera que los datos personales son cualquier información concerniente a una persona física identificada o identificable.[56] Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.[57]

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante "LGPDPPSO") señala que los datos sensibles son:

> Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

En este sentido, el uso de TRF en el espacio público implica el tratamiento de datos sensibles, por lo cual, constituye un tratamiento de datos personales sensibles; es decir, interfiere de manera significativa en el ejercicio del derecho a la privacidad y a la protección de datos personales.

La LGPDPPSO establece que tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito de la persona titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación. Sin embargo, el uso de TRF recaba datos biométricos de manera furtiva y remota, lo cual impide que las personas puedan dar un consentimiento real sobre el tratamiento de sus datos.

//* ----------

54/ Corte IDH. Caso Escué Zapata Vs. Colombia. Fondo, Reparaciones y Costas. Sentencia de 4 de julio de 2007. Serie C No. 165, párr. 95; Caso Tristán Donoso vs. Panamá. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 27 de enero de 2009. Serie C No. 193, párr. 55; y Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 113.

55/ Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 115.

56/ Artículo 3. Fracción: Para los efectos de la presente Ley se entenderá por: Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

57/ *Idem*.

Las autoridades estatales utilizan estas formas de vigilancia para hacer identificación biométrica de manera remota, pues permite identificar (o asumir una identificación) desde la distancia en lugares público. Este uso se hace de manera encubierta sin que las personas tengan conocimiento de ello. Las personas no tienen la oportunidad de decidir si quieren que sus datos biométricos sean recolectados y almacenados en bases de datos para después ser sometidas a búsquedas y escrutinios constantes de manera permanente.[58] Por lo tanto, la vigilancia y recolección de los datos personales de manera remota, encubierta y masiva supone una trasgresión a la expectativa de privacidad que las personas gozan en el ámbito público.

Otra forma en la que el sistema de reconocimiento facial vulnera la protección de datos personales es el riesgo de la vulneración de las bases de datos donde se recolectan y almacenan datos biométricos y los datos generados a partir de la operación del sistema.

Con la proliferación de bases centralizadas de datos biométricos utilizadas por gobiernos, el Alto Comisionado de las Naciones Unidas se ha pronunciado sobre los peligros del uso de datos biométricos en bases centralizadas de datos[59] –como el robo de identidad, la proliferación de la vigilancia ilegal y las afectaciones a sectores vulnerables–, por lo que ha instado a que los Estados evalúen estas medidas bajo los principios de necesidad y proporcionalidad, así como las garantías jurídicas y procesales necesarias.

Las bases de datos biométricos contienen información que está vinculada permanentemente con las personas. Cualquier transgresión en estas bases de datos puede resultar daños irreparables para las víctimas de robo de identidad ya que, una vez sustraída esa información, no puede recuperarse y las personas podrían verse afectadas por el resto de sus vidas.[60]

Afectaciones a la libertad de expresión y de reunión pacífica

El uso de TRF en el espacio público también afecta la libertad de expresarnos sin temor a represalias. Existe una estrecha relación entre el derecho a la intimidad, el derecho a la libertad de expresión y el derecho a la reunión pacífica. Las personas muestran su rostro al salir a la calle a realizar su vida privada y al participar en la vida pública, sin embargo, habrá algunas que prefieren el anonimato en la esfera pública para poder expresarse de manera libre para evitar represalias.[61]

//* ----------

58/ Boyd, Dannah. “The Future of Privacy: How Privacy Norms can Inform Regulation”. 29 de octubre de 2019. Disponible en: https://www.danah.org/papers/talks/2010/PrivacyGenerations.html

59/ Alto Comisionado de las Naciones Unidas para los Derechos Humanos. “El derecho a la privacidad en la era digital” A/HRC/39/29 https://undocs.org/es/A/HRC/39/29

60/ Murgia, Madhumita. “The insidious threat of biometrics”. Financial Times.. Publicado el 18 de febrero de 2019. https://www.ft.com/content/cdf0d52a-c2de-11e9-a8e9-296ca66511c9

61/ Voto de la Jueza Sotomayor de la Suprema Corte de Justicia de Estados Unidos en el caso de United States vs Jones. 132 S. Ct 945(J. Sotomayor concurrente) Consulta en: https://www.law.cornell.edu/supremecourt/text/10-1259#writing-10-1259_CONCUR_4

La libertad de expresión es la piedra angular de una sociedad democrática y una condición esencial para que esté suficientemente informada,[62] por lo cual la Corte IDH establece que las garantías de la libertad de expresión están diseñadas para ser las más generosas y reducir al mínimo las restricciones a la libre expresión de ideas.[63]

El derecho a la libertad de expresión comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole. En este sentido, tanto la Corte IDH[64] como la SCJN[65] han precisado que el conocimiento de la opinión ajena o de la información de la que disponen otros resulta ser tan importante como el derecho a difundir la propia.

De igual forma, el derecho a la libertad de expresión posee dos dimensiones: una individual y una social. Esta doble dimensión implica que nadie pude ser impedido de manifestar sus ideas como derecho individual; pero también supone un derecho colectivo que tienen las personas para recibir cualquier tipo de información y conocer la pluralidad de expresiones en la sociedad.[66]

Adicionalmente, el derecho a la libertad de expresión no solo protege la expresión oral, escrita o visual. Para la Declaración de Principios sobre Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (en adelante, CIDH), este derecho protege las expresiones humanas "en todas sus formas y manifestaciones".[67]

La libertad de expresión se encuentra sensiblemente ligada al derecho a privacidad en tanto una injerencia indebida en la intimidad de las personas puede limitar en forma tanto directa como indirecta el libre intercambio y evolución de ideas. Así lo ha expresado el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión de la ONU, al señalar que: "las restricciones al anonimato de las comunicaciones, por ejemplo, tienen un efecto intimidatorio en las víctimas de todas las formas de violencia y abuso, que podrían ser renuentes a denunciarlas por temor a la doble victimización".[68]

En ese mismo sentido, la Relatoría Especial para la Libertad de Expresión de la CIDH ha señalado que:

//* ----------

62/ Corte IDH. Serie C No. 73. Caso "La Última Tentación de Cristo" (Olmedo Bustos y otros) vs. Chile. Fondo y Reparaciones y Costas. Sentencia de 5 de febrero de 2001, párr. 68 y SCJN. 1ª Sala. Amparo Directo 28/2010. Sentencia de 23 de noviembre de 2011.

63/ Corte IDH. Serie A No. 5. La Colegiación Obligatoria de Periodistas (Arts. 13 y 29 de la Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985, párr. 52.

64/ Corte IDH. Serie A No. 5. La Colegiación Obligatoria de Periodistas (Arts. 13 y 29 de la Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985, párr. 32.

65/ SCJN. 1ª Sala. Amparo en Revisión 1595/2006. Sentencia de 29 de noviembre de 2006.

66/ Corte IDH. Serie C No. 107. Caso Herrera Ulloa vs. Costa Rica. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 2 de julio de 2004, párr 108; Serie C No 111. Caso Ricardo Canese vs. Paraguay. Fondo, Reparaciones y Costas. Sentencia de 31 de agosto de 2004, párr.77.; y I Serie C No. 74. Caso Ivcher Bronstein vs. Perú. Reparaciones y Costas. Sentencia de 6 de febrero de 2001, párr. 146.

67/ CIDH. Declaración de Principios sobre Libertad de Expresión. Aprobada por la Comisión Interamericana de Derechos Humanos en octubre de 2000, en el 108 período ordinario

68/ Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40 17 de abril de 2013

> Los Estados deben evitar la implementación de cualquier medida que restrinja, de manera arbitraria o abusiva, la privacidad de los individuos (...) entendida en sentido amplio como todo espacio de intimidad y anonimato, libre de amedrentamiento y de represalias, y necesario para que un individuo pueda formarse libremente una opinión y expresar sus ideas así como buscar y recibir información, sin ser forzado a identificarse o a revelar sus creencias y convicciones o las fuentes que consulta.[69]

Por su parte, el derecho a la reunión pacífica protege la organización o participación de las personas en una reunión con el fin de realizar la transmisión de una posición sobre un asunto en particular o el intercambio de ideas. La reunión también puede tener la intención de sostener o afirmar solidaridad o identidad de grupo.[70]

El Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación de la ONU ha expresado que dichas reuniones: "desempeñan un papel muy dinámico en la movilización de la población y la formulación de sus reclamaciones y aspiraciones, pues facilitan la celebración de eventos y, lo que es más importante, ejercen influencia en la política pública de los Estados".[71]

En la Observación General No. 37, el Comité de Derechos Humanos (en adelante, CDH) ha establecido, respecto del derecho a la reunión pacífica, que los Estados tienen deberes positivos y negativos para cumplir su obligación de respetar y garantizar las reuniones pacíficas.[72] Entre ellos, se encuentra el abstenerse de realizar interferencias injustificadas, por lo cual no pueden establecer restricciones a menos que la autoridad justifique que cumpla los requisitos de legalidad, necesidad y proporcionalidad[73] en los términos posibles para restricciones enumeradas en el artículo 21 del Pacto Internacional de Derechos Civiles y Políticos.

Igualmente, las personas que protestan tienen derecho a tomar las medidas necesarias para manifestarse de manera anónima. La protesta anónima es parte esencial de los elementos de una reunión pacífica pues sirve para evitar represalias o proteger la privacidad en el contexto de las tecnologías de vigilancia.[74]

En este sentido, el derecho a la libertad de expresión y de reunión pacífica también se encuentran íntimamente ligados en tanto, como se ha reconocido, la protesta es una forma de

//* ----------

69/ CIDH. Libertad de Expresión e Internet. Párr. 132.

70/ Comité de Derechos Humanos. Observación General no. 37. Artículo 21: derecho a la reunión pacífica. 27 de julio de 2020, C/20/27, párr. 12.

71/ Consejo de Derechos Humanos, Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Maina Kiai, 21 de mayo de 2012, A/HRC/20/27, párr. 24

72/ Comité de Derechos Humanos. Observación General no. 37. Artículo 21: derecho a la reunión pacífica. 27 de julio de 2020, C/20/27, párr. 23

73/ *Ídem.* par. 36

74/ *Ídem.* para. 60-63

acción individual o colectiva dirigida a expresar ideas, visiones o valores de disenso, oposición, denuncia o reivindicación.[75]

Adicionalmente, como ha sido mencionado anteriormente, también existe una íntima relación entre el derecho a la privacidad y el derecho de reunión pacífica. Al respecto el CDH ha señalado que "el solo hecho de que una reunión se lleve a cabo en público no significa que la privacidad de los participantes no puede ser violada. El derecho a la privacidad puede ser infringido, por ejemplo, por reconocimiento facial y otras tecnologías que pueden identificar a los participantes en una multitud".[76]

Igualmente, el CDH ha establecido que la recolección masiva de datos personales por parte de las autoridades no debe resultar en una supresión de derechos o crear un efecto inhibidor para ejercerlos. La recolección de información, ya sea por entidades públicas o privadas, obtenidas por vigilancia o intervención de comunicaciones, así como la forma en la que se recolectó, compartió, retuvo y accedió, debe realizarse con estricta conformidad con los estándares internacionales de derechos humanos.

El CDH hace especial énfasis en que estos datos nunca deben ser utilizados para intimidar o acosar participantes –o participantes en potencia– de la reunión; así como también establece que dichas prácticas deberán de estar reguladas por un marco legal y sujeto a escrutinio.

En 2023, el Tribunal Europeo de Derechos Humanos consideró que Rusia violó los derechos a la privacidad y libertad de expresión al recolectar datos biométricos de una persona durante una protesta pacífica.[77] El TEDH resolvió que el procesamiento de los datos biométricos del ciudadano no cumplían con los requisitos mínimos de necesidad y proporcionalidad, por lo que la sentencia establece que las medidas que realizó el gobierno ruso en contra de ciudadano habían sido altamente intrusivas y habían violentado su derecho a la privacidad y libertad de expresión.

La TRF en espacios públicos supone la operación de un sistema masivo, permanente, ineludible, indiscriminado y altamente invasivo de videovigilancia con reconocimiento facial, capaz de identificar a personas en el espacio público y generar un registro de hora, fecha y ubicación de dichas detecciones asociadas a una persona, e incluso potencialmente de su estado de ánimo. El uso de esta tecnología constituye una grave interferencia con los derechos a la libertad de expresión y de reunión, en conexión con el derecho a la privacidad y protección de datos personales.

De la misma manera, el software de reconocimiento facial puede, de manera encubierta, remota y masiva, capturar e identificar imágenes de no solamente el rostro de la persona,

//* ----------

75/ Relatoría Especial para la Libertad de expresión. "Protesta y Derechos Humanos" CIDH OEA/Ser.L/V/II CIDH/RELE/INF.22/19 septiembre 2019. Consulta en: http://www.oas.org/es/cidh/expresion/publicaciones/ProtestayDerechosHumanos.pdf

76/ Comité de Derechos Humanos. Observación General no. 37. Artículo 21: derecho a la reunión pacífica. 27 de julio de 2020, C/20/27, párr. 62.

77/ Corte Europea de Derechos Humanos. Glukhin vs Rusia. Aplicación 11519/20. Resuelto el 4 de octubre de 2023.

sino su forma de vestir e incluso con quién se encuentra acompañada.[78] Esto propicia la vigilancia masiva y encubierta de las personas en el espacio público, lo que provoca un ambiente hostil que inhibe el ejercicio de derechos humanos como la libertad de expresión y de reunión pacífica. La noción de que el gobierno pueda estar observando a cada segundo generará un efecto paralizante en los gobernados que reprime su derecho a la libre expresión.

La vigilancia masiva del espacio público con tecnologías de reconocimiento facial impide que las y los ciudadanos puedan realizar sus actividades diarias de manera anónima. El CDH ha establecido que el anonimato de los participantes siempre debe ser permitida a menos que su conducta resulte en un hecho delictivo.[79] El anonimato es un elemento esencial del proceso expresivo y del derecho a la reunión pacífica, sirve para contrarrestar represalias o proteger la privacidad de los manifestantes.

Afectaciones a los derechos a la presunción de inocencia y debido proceso

Una de las principales justificaciones para el uso de la TRF es la protección de la seguridad pública y la procuración de justicia. El software de reconocimiento facial tiene como objetivo la identificación de personas para que puedan ser sujetas a procesos de investigación y sanción en materia penal.

Sin embargo, la TRF implica el tratamiento masivo, indiscriminado, encubierto y permanente de datos personales sensibles de personas captadas por dicho sistema. La mayoría de estas personas no se encuentran en ningún supuesto que justifique la interferencia en sus derechos y que no son relevantes ni guardan relación con ninguna investigación criminal. Esto implica una transgresión grave al principio de presunción de inocencia.

La tecnología de reconocimiento facial viola la presunción de inocencia en su modalidad de tratamiento procesal. En el sistema jurídico mexicano, el principio de presunción de inocencia tiene una vertiente donde todas las personas deben de ser tratadas como inocentes hasta que se compruebe lo contrario. La Primera Sala de la SCJN ha establecido que “la regla de tratamiento” se manifiesta en la forma en la que debe tratarse a una persona sometido a proceso penal comporta como inocente en tanto no se declare su culpabilidad por virtud de una sentencia condenatoria.[80]

Los sistemas con capacidad de reconocimiento facial realizan tratamientos de datos personales sensibles que le dan un trato equivalente al de “sospechoso” a todas las personas

//* ----------

78/ Lynch, Jennifer, What Facial Recognition Technology Means for Privacy and Civil Liberties (July 18, 2012). Disponible en SSRN: http://dx.doi.org/10.2139/ssrn.2134497

79/ Consejo de Derechos Humanos. Observación General no. 37. Artículo 21: derecho a la reunión pacífica. 27 de julio de 2020, C/20/27, párr. 60

80/ 1a./J. 24/2014 (10a.) Primera Sala. Registro: 2006092. Gaceta del Semanario Judicial de la Federación p.497

81/ Garvie Clare, Bedoya Alvaro and Frankle Jonathan. “The Perpetual Line-Up: Unregulated-Police Face Recognition in America” Georgetown Law: Center on Privacy and Technology.18 de Octubre de 2016. Consultado el 7 de julio de 2021 en: perpetuallineup.org

que transiten la vía pública, independientemente de que hayan participado en la comisión un hecho delictivo o no. La manera indiscriminada en la que operan las TRF produce una "línea policial" perpetua[81] donde todas las personas se tendrán como sospechosas al hacer la referencia cruzada con la imagen de quien se está investigando.

Lo anterior genera un riesgo impermisible de abusos derivado de las inherentes fallas y deficiencias del sistema. Inclusive, dichos abusos se han materializado de manera frecuente en jurisdicciones en las que sistemas similares han sido puestos en operación. Por ejemplo, el 24 de junio de 2020, la policía de la ciudad de Detroit, en Estados Unidos, arrestó a Robert Julian-Borchank, un hombre afroamericano inocente. La policía alegó que cometió una serie de delitos debido a que el algoritmo de reconocimiento facial señalaba la coincidencia entre el rostro de Williams y una foto borrosa que claramente correspondía a otra persona.[82]

El sistema de reconocimiento facial había cometido un error, mismo que fue documentado en un estudio federal,[83] dentro de los que se encuentra la empresa que proporcionó la tecnología del presente caso, debido a un sistema sesgado que identificaba incorrectamente a personas afroamericanas y asiáticas de 10 a 100 veces más que rostros caucásicos.[84]

Como expusimos anteriormente, el sistema no señala de manera categórica sobre la identidad de una persona, sino que hace un estimado porcentual de las similitudes entre los rostros comparados. Una persona puede estar simplemente en el lugar y momento equivocado o encajar en un fenotipo o contar con una característica física que haya sido detectada por un algoritmo defectuoso para ser señalada de manera equivocada por el sistema.[85]

Afectaciones al derecho a la igualdad y no discriminación

La TRF es imprecisa y altamente susceptible a errores. Estas imprecisiones impactan de manera desigual a grupos vulnerables, en específico a personas de color, personas indígenas, mujeres o personas de la comunidad LGBTTTIQ+, lo que propicia la discriminación y vulnera sus derechos a la igualdad y no discriminación.

La discriminación, ya sea respecto de normas o actos, puede acontecer tanto de manera directa como indirecta. La jurisprudencia de la SCJN establece que la discriminación indirecta significa que las leyes, las políticas o las prácticas públicas o privadas son neutras

//* ----------

82/ Wrongfully Accused by an Algorithm https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html#click=https://t.co/KxKC81AEFV

83/ Groher Patrick, Ngan Mei, Hanoaka Kayee. "Face Recognition Vendor Test Part: 3 Demographic Effects" Link: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

84/ Many facial Recognition Systems are biased, Says U.S Study https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

85/ Lynch, Jennifer, What Facial Recognition Technology Means for Privacy and Civil Liberties (July 18, 2012). Available at SSRN: https://ssrn.com/abstract=2134497 or http://dx.doi.org/10.2139/ssrn.2134497

en apariencia, pero afectan desproporcionadamente a personas o grupos en situación de desventaja histórica justo en razón de esa desventaja,[86] en comparación de otros en una situación análoga[87] sin que exista para ello una justificación objetiva y razonable.[88]

La Corte Interamericana de Derechos Humanos ha precisado que el principio de derecho imperativo de protección igualitaria y efectiva de la ley y no discriminación determina que los Estados "deben abstenerse de producir regulaciones discriminatorias o que tengan efectos discriminatorios en los diferentes grupos de una población al momento de ejercer sus derechos".[89]

La SCJN también ha manifestado que es necesario introducir factores contextuales o estructurales en el análisis de la discriminación para poder establecer que una norma o política pública sí genera un efecto discriminatorio en la persona, aunque aparente ser neutral. Entre estos factores se ubican las relaciones de subordinación en torno al género, la identidad sexo-genérica, la orientación sexual, la clase o la pertenencia étnica; las prácticas sociales y culturales que asignan distinto valor a ciertas actividades –en tanto son realizadas por grupos históricamente desaventajados– y las condiciones socioeconómicas.[90] Estos factores condicionan que una ley o política pública finalmente provoque una diferencia de trato irrazonable, injusto o injustificable de acuerdo con la situación que ocupen las personas dentro de la estructura social.[91]

El software de reconocimiento facial se ostenta la mayoría de las veces como una tecnología neutra que no toma en consideración categorías como género o color de piel. Sin embargo, afecta desproporcionadamente a grupos históricamente oprimidos por dos principales factores:

- El primer factor es la subrepresentación de rostros de color, personas con rasgos asiáticos, de pueblos originarios o personas no heteronormadas en las bases de datos utilizadas en el entrenamiento de los algoritmos de reconocimiento facial.[92]

//* ----------

86/ Acción de Inconstitucionalidad 8/2014. Aprobado por mayoría de votos. Ponente: Margarita Beatriz Luna Ramos. Encargado del engrose: Alfredo Gutiérrez Ortiz Mena. Secretaria: Karla I. Quintana Osuna. p. 89 par.71 De esta sentencia derivó la Tesis aislada P. VII/2016 (10a.) emitida por el Pleno de la SCJN de rubro: "DISCRIMINACIÓN POR OBJETO Y POR RESULTADO. SU DIFERENCIA." Registro 2012597

87/ AD 9/2018 p. 32

88/ Tesis 1ª. XLIV/2014 (10a.), emitida por la Primera Sala de esta Suprema Corte de rubro y texto: "DERECHO HUMANO A LA IGUALDAD JURÍDICA. DIFERENCIAS ENTRE SUS MODALIDADES CONCEPTUALES

89/ Cfr. Caso Artavia Murillo y otros ("fecundación in vitro") vs. Costa Rica. *Fondo, Reparaciones y Costas.* Sentencia de 28 de septiembre de 2012. Página 134. Párrafos 285 y 286.

90/ Acción de Inconstitucional 8/2014 op cit. 78 p. 90 par. 74

91/ Id. citando a Saba, Roberto, "Desigualdad estructural", en Roberto Gargarella y Marcelo Alegre, El derecho a la igualdad. Aportes para un constitucionalismo igualitario, Buenos Aires, Lexis Nexis, 2007 y Serrano García, Sandra et al. "Herramientas para una comprensión

92/ Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

- El segundo factor es el hecho de que inclusive con la utilización de bases de datos más balanceadas en el entrenamiento de algoritmos, es más difícil para los sistemas reconocer los tonos de piel más oscuros.[93]

Evidencia científica sostiene que muchas de estas clasificaciones son realizadas utilizando métodos pseudocientíficos o con sesgos raciales[94] que generan estos efectos desproporcionados. Simone Browne acuñó el término de *epidermización digital* al ejercicio de poder que realiza la mirada incorpórea de las herramientas de vigilancias que sirve para alienar al sujeto observado, al producir una "verdad" sobre su cuerpo y sus identidades.[95]

Browne argumenta que la epidermización digital es la razón por la cual ocurre este efecto desproporcionado, ya que el prejuicio sistemático establece la blanquitud como norma y prototípica y las personas racializadas son víctimas de la epidermización digital.[96]

Por ejemplo, existen casos donde se entrena al algoritmo para detectar personas con una alta probabilidad de criminalidad a partir de bases de datos penales de una zona geográfica con una mayor población de personas racializadas. En contraste, el reconocimiento de personas caucásicas suele tener tasas muy pequeñas de falsos positivos en comparación con los demás grupos demográficos, a pesar de encontrarse en la misma base, por las condiciones que afectan la objetividad de los sistemas de reconocimiento facial.[97]

Así mismo, las TRF se crean a partir de la concepción binaria del género que implantan los programadores al sistema. Esto provoca que cuerpos transgénero se vean poco representados a comparación de rostros y cuerpos cisgénero en la base de datos que alimenta el software de reconocimiento facial.[98]

Esta situación pone en estado de indefensión a todas aquellas personas transgénero y personas no binaries que pasen frente a cámaras de reconocimiento facial.[99] Por lo tanto, la tasa de error en la que pueden incurrir es más alta, lo que puede traducirse en que se le considere como una persona sospechosa en alguna investigación. Esto pone en peligro agravado su integridad física, en tanto se ha demostrado que las personas transgénero o

//* ----------

93/ B. F. Klare, M. J. Burge, J. C. Klontz, R. W. Vorder Bruegge and A. K. Jain, "Face Recognition Performance: Role of Demographic Information," in *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1789-1801, Dec. 2012, doi: 10.1109/TIFS.2012.2214212. https://ieeexplore.ieee.org/document/6327355

94/ Browne, Simone, *Dark matters: on the surveillance of blackness*. Durham: Duke University Press, 2015.

95/ Browne, 135.

96/ Simone Browne, "Digital Epidermalization: Race, Identity and Biometrics", *Critical Sociology* 36, núm. 1 (enero de 2010): 133–35, https://doi.org/10.1177/0896920509347144

97/ Big Brother Watch. " Face Off: The lawless growth of facial recognition in UK policing" Mayo 2018. Consulta en: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

98/ Cfr. O. Keyes The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition. University of Washington, USA. https://ironholds.org/resources/papers/agr_paper.pdf#page=19&zoom=100,0,710

99/ Gault Matthew. "Facial Recognition Software Regularly Misgenders Trans People" Febrero 2019. https://www.vice.com/en_us/article/7xnwed/facial-recognition-software-regularly-misgenders-trans-people Visitado el 15/04/20

no binaries son más susceptibles de ser víctimas de violencia y detenciones arbitrarias por parte de la policía.[100]

En conclusión, si bien la tecnología de reconocimiento facial no hace categorías específicas para dar un trato diferenciado a las personas, los resultados de este sistema tienen un impacto desproporcionado en estos grupos vulnerables, derivado de una falta de inclusividad en el desarrollo de esta tecnología, así como exhibe los sesgos implícitos[101] con los que muchos de las y los programadores cuentan y trasladan a estos algoritmos.

Por ello, cabe concluir que el uso de reconocimiento facial se traduce en una discriminación indirecta al generar un impacto desproporcionado sobre grupos vulnerables como personas con discapacidad, racializadas, indígenas, mujeres y personas de la comunidad LGBTTIQ+.

//* ----------

100/ Stotzer, R. L. (2014). Law enforcement and criminal justice personnel interactions with transgender people in the United States: A literature review. Aggression and Violent Behavior, 19(3), 263–277. doi:10.1016/j.avb.2014.04.012

101/ Barocas, Solon and Selbst, Andrew D., Big Data's Disparate Impact (2016). 104 California Law Review 671 (2016), Disponible en SSRN: https://ssrn.com/abstract=2477899 or http://dx.doi.org/10.2139/ssrn.2477899. Véase también Hellman, Deborah, Measuring Algorithmic Fairness (July 11, 2019). Virginia Public Law and Legal Theory Research Paper No. 2019-39, Virginia Law and Economics Research Paper No. 2019-15, Virginia Law Review, Forthcoming, https://ssrn.com/abstract=3418528

CAP.02\\

RECONOCIMIENTO FACIAL EN CIUDADES DE MÉXICO: LOS CASOS DE COAHUILA Y AGUASCALIENTES

En México, los estados de Coahuila y Aguascalientes ya han empezado a implementar las TRF en sus ciudades. A pesar de todas los riesgos que suponen las TRF para los derechos humanos, los gobiernos han implementado esta tecnología bajo la justificación de mejorar la seguridad pública de los estados.

En este capítulo analizaremos los casos del uso de software de reconocimiento facial implementado en las ciudades dentro de los estados de Coahuila y Aguascalientes. Hemos documentado desde las cámaras utilizadas, la falta de seguridad jurídica en su uso, hasta las afectaciones que han generado en los derechos de su ciudadanía.

SISTEMA DE VIDEO INTELIGENCIA PARA LA SEGURIDAD: EL RECONOCIMIENTO FACIAL EN COAHUILA

El 2 de abril de 2019, el entonces gobernador del Estado de Coahuila, Miguel Riquelme, presentó el "Sistema de Video Inteligencia para la Seguridad", el cual incluyó la instalación de cerca de mil 300 cámaras de vigilancia,[102] un tercio de estas con capacidades de reconocimiento facial y con reconocimiento de placas.[103] Las cámaras fueron instaladas en 370 puntos de las once ciudades más pobladas de Coahuila: Acuña, Monclova, Arteaga, Arizpe, Francisco I. Madero, Frontera, Piedras Negras, Saltillo, San Pedro y Torreón.

El costo estimado del "sistema de video inteligencia" –según declaraciones del gobierno de Coahuila– sería de 600 millones de pesos.[104] Dicho presupuesto comprendió la compra del sistema de vigilancia y la modernización de varios de los Centros de Comunicaciones, Cómputo, Control y Comando, los cuales son los encargados de operar el sistema de vigilancia del espacio público que existen en las mencionadas ciudades anteriormente.

//* ----------

102/ El Universal. "Preparan cámaras de vigilancia con reconocimiento facial en Coahuila". Accedido 28 de mayo de 2024. https://www.eluniversal.com.mx/estados/preparan-camaras-de-vigilancia-con-reconocimiento-facial-en-coahuila/

103/ Sánchez, Esmeralda. "Coahuila. Cámaras de seguridad tendrán interconexión". Grupo Milenio, 18 de julio de 2021. https://www.milenio.com/policia/coahuila-camaras-de-seguridad-tendran-interconexion

104/ Flores, Nancy. "En México operan tres sistemas de vigilancia con reconocimiento facial". Contralínea (blog), 12 de noviembre de 2021. https://contralinea.com.mx/interno/semana/en-mexico-operan-tres-sistemas-de-vigilancia-con-reconocimiento-facial/

La actual administración plantea ampliar el sistema de TRF. El 4 de diciembre de 2023, el gobernador de Coahuila, Manolo Jiménez Salinas, presentó como parte de sus primeros 100 días de gobierno, el plan de la implementación de arcos de revisión en los puntos de carreteras a la entrada de entrada al estado de Coahuila, los cuales incluirán cámaras con capacidades de revisión de matrículas así como de reconocimiento facial. No hay más información pública que detalle las capacidades de dicho sistema o la forma en que será utilizado.

PREOCUPACIONES EN TORNO AL SISTEMA DE RECONOCIMIENTO FACIAL EN COAHUILA

Según declaraciones del gobernador Jiménez Salinas, hechas durante la presentación del sistema, se busca la interoperabilidad con las bases de datos de la Plataforma México y del Instituto Nacional Electoral para llevar a cabo el proceso de identificación mediante reconocimiento facial.[105] Luis Campos, director de la plataforma C4 del Estado de Coahuila durante el mandato de Riquelme, declaró posteriormente en una entrevista que la capacidad computacional del sistema actual imposibilita el uso de bases de datos con la magnitud de las anteriormente mencionadas para llevar a cabo reconocimiento facial en tiempo real.[106]

El uso de bases de datos masivas, como las de la Plataforma México y del Instituto Nacional Electoral, plantean preocupaciones adicionales en materia de afectaciones a la privacidad, puesto que su uso permite la identificación de un altísimo porcentaje de la población. Esto significa, en la práctica, el fin del anonimato en el espacio público como lo conocemos, así como una violación del principio de consentimiento para el cual originalmente fueron obtenidos dichos datos.

La ubicación de las cámaras de vigilancia instaladas como parte de este proyecto levantan sospechas sobre su verdadero objetivo. De acuerdo a una respuesta de la Secretaría de Seguridad a una solicitud de acceso a la información realizada por R3D, la ubicación fue determinada en relación a la ubicación de la mayoría de los delitos.[107] Sin embargo, una investigación periodística encontró que la localización de las cámaras de vigilancia no guarda relación con los índices delictivos en el estado de Coahuila.[108] Por ejemplo, de todas las regiones en donde se instalaron cámaras con TRF, apenas una coincide con el aumento de índices delictivos a partir de 2018.

//* ----------

105/ Pérez Villoro, Federico y Robles, Paloma . Quinto Elemento Lab. "Vigilancia Biométrica: El Tortuoso Camino de Coahuila Hacia El Reconocimiento Facial". Accedido 28 de mayo de 2024. https://quintoelab.org/project/vigilancia-biometrica-reconocimiento-facial-coahuila

106/ Pérez Villoro, Federico y Robles, Paloma . Quinto Elemento Lab. "Vigilancia Biométrica: El Tortuoso Camino de Coahuila Hacia El Reconocimiento Facial". Accedido 28 de mayo de 2024. https://quintoelab.org/project/vigilancia-biometrica-reconocimiento-facial-coahuila

107/ Respuesta a solicitud de acceso a la información 887620 realizada por R3D a la Secretaría de Seguridad Pública de Coahuila. https://drive.google.com/file/d/1iKxf1zGFhyLsVrLKykjmHsGz0m_UXupX/view

108/ Pérez Villoro, Federico y Robles, Paloma . Quinto Elemento Lab. "Vigilancia Biométrica: El Tortuoso Camino de Coahuila Hacia El Reconocimiento Facial". Accedido 28 de mayo de 2024. https://quintoelab.org/project/vigilancia-biometrica-reconocimiento-facial-coahuila

Otra de las preocupaciones en torno a este sistema surge de la falta de transparencia y rendición de cuentas. El gobierno del estado de Coahuila ha mantenido en opacidad documentos relacionados a la compra del sistema de videovigilancia con reconocimiento facial, así como demás información relacionada a capacidades del sistema, cámaras, software o equipos, la ubicación de las cámaras de vigilancia, así como el umbral de probabilidad que será utilizado para determinar la identificación de una persona.

Por otra parte, es preocupante que autoridades de otros órdenes dentro del gobierno –además de la Secretaría de Seguridad Pública– tengan acceso al sistema de reconocimiento facial. Un video de la presentación del C4 de la Laguna, el centro de operación del sistema de vigilancia de esta región, muestra cómo la operación de este corre en parte a manos del Ejército y de la Guardia Nacional, además de la Dirección de Seguridad Pública Municipal y de la Fiscalía de Justicia del Estado de Coahuila.[109]

La falta de certeza sobre el uso del sistema complica la detección de potenciales abusos, manteniéndolos en la impunidad; además, imposibilita el escrutinio público sobre la efectividad de una costosa iniciativa que tiene impactos profundos en la privacidad de las personas. Esto es especialmente preocupante dado el contexto de abuso que existe en torno al uso de herramientas de vigilancia que prevalece en el país para perseguir a activistas y periodistas, como lo muestran diversas investigaciones.[110]

Vigilancia sin fundamento legal

En mayo del año 2019, el gobernador Riquelme presentó una iniciativa en el Congreso del Estado para regular el uso de reconocimiento facial. Según esta propuesta, el sistema de vigilancia adquirido por el Estado de Coahuila contaría con capacidades de reconocimiento facial, de placas, análisis flujo de tránsito, videovigilancia, e inclusive detección de emociones.[111] Dicha iniciativa no fue discutida, quedando en el olvido.

Un año después, en abril del año 2021, Rodolfo Walss Aurioles, legislador del Partido Acción Nacional, presentó una nueva iniciativa sobre la regulación del uso de cámaras de reconocimiento facial en el Estado de Coahuila.[112] Hasta la fecha de la publicación del presente informe, esa iniciativa no había sido discutida.

//* ----------

109/ Video de la inauguración del C4 en Matamoros, Coahuila: https://r3d.mx/wp-content/uploads/GOBERNADOR%20MIGUEL%20RIQUELME%20INAUGURA%20MODERNIZACI%C3%93N%20DEL%20C4%20EN%20MATAMOROS.mp4

110/ R3D: Red en Defensa de los Derechos Digitales. "#GobiernoEspía: vigilancia sistemática a periodistas y defensores de derechos humanos en México". R3D: Red en Defensa de los Derechos Digitales (blog), 19 de junio de 2017. https://r3d.mx/2017/06/19/gobierno-espia/ y R3D: Red en Defensa de los Derechos Digitales. "Ejercito Espía | Capítulo I". Accedido 28 de mayo de 2024. https://ejercitoespia.r3d.mx/ejercito-espia/

111/ Miguel Ángel Riquelme, Iniciativa con Proyecto de Decreto por el que se crea la Ley que Regula el Uso de las Cámaras de Video Vigilancia y Video Inteligencia para la Seguridad Pública del Estado de Coahuila de Zaragoza. 23 de diciembre de 2020. https://www.congresocoahuila.gob.mx/transparencia/03/Iniciativas-2018-2020/20201223_070_Ejec.docx

112/ Walss Aurioles, Rodolfo Gerardo. Iniciativa con Proyecto de Decreto por el que se crea la Ley que Regula la Videovigilancia en el Estado de Coahuila de Zaragoza. 27 de abril de 2021. https://www.congresocoahuila.gob.mx/transparencia/03/Iniciativas-2021-2023/20210427_025_PAN.docx

En respuestas a solicitudes de acceso a la información realizadas por R3D entre los años 2020 y 2022, el gobierno de Coahuila declaró que el sistema de reconocimiento facial se encontraba en fase de prueba. Según declaraciones del director de la plataforma C4, las pruebas del sistema de TRF se han efectuado utilizando "listas de excepción", las cuales incluyen datos de personas prófugas de la ley, así como de personas desaparecidas.[113]

Así mismo, en respuestas a solicitudes de acceso a la información, la Secretaría de Seguridad Pública reservó toda la información relacionada a los procesos de elaboración, mantenimiento, gestión y evaluación de las bases de datos con las que se lleva a cabo el reconocimiento facial,[114] por lo que no es posible tener certeza sobre el tipo de bases de datos que se han utilizado en la utilización del sistema.

En la entrega de la remodelación de C4 de Matamoros, el entonces gobernador Riquelme declaró que "el sistema de video inteligencia en su fase de pruebas ha resuelto 8 homicidios y alrededor de 60 delitos del fuero común". No queda claro, qué entiende el gobierno de Coahuila por "prueba", si el sistema ya ha sido utilizado para identificar a personas inocentes y a supuestos sospechosos en el espacio público.

Según la Secretaría de Seguridad del Estado de Coahuila, actualmente la Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública es el fundamento jurídico que sustenta la operación del sistema de reconocimiento facial en el estado. Esta fue publicada en 2016,[115] en un momento en el que la vigilancia masiva mediante reconocimiento facial no se comercializaba como ocurre hoy en día. Dicha norma ni siquiera menciona cuestiones relacionadas al tema de tratamiento de datos biométricos o el proceso de reconocimiento facial.

No existe un fundamento legal para la utilización del sistema si este incluye reconocimiento facial ni el ordenamiento legal que existe actualmente asegura el correcto tratamiento de los datos personales que son captados. De manera más preocupante, el sistema planteado es inconstitucional, al permitir el ejercicio de vigilancia masiva.

La relación comercial con Dahua, empresa en lista negra

Dahua, la empresa proveedora del Sistema de Video Inteligencia, su instalación y entrenamiento para su utilización aparece en una lista negra del Departamento de Defensa de Estados Unidos por ser utilizadas para vigilar y oprimir minorías en la provincia de Xinjiang

//* ----------

113/ Pérez Villoro, Federico y Robles, Paloma . Quinto Elemento Lab. "Vigilancia Biométrica: El Tortuoso Camino de Coahuila Hacia El Reconocimiento Facial". Accedido 28 de mayo de 2024. https://quintoelab.org/project/vigilancia-biometrica-reconocimiento-facial-coahuila

114/ Respuesta a solicitud de acceso a la información 887620 realizada por R3D a la Secretaría de Seguridad Pública de Coahuila. https://r3d.mx/wp-content/uploads/Respuesta-Coahuila-887620.pdf

115/ Respuesta a solicitud de acceso a la información 887620 realizada por R3D a la Secretaría de Seguridad Pública de Coahuila. https://r3d.mx/wp-content/uploads/Respuesta-Coahuila-887620.pdf

en China.[116] El uso de dichos sistemas de vigilancia en el espacio público ha aportado a la violación masiva y sistemática de los derechos de personas musulmanas en esta región. Más de 13 millones de personas han sido objeto de detención arbitraria y opresión por parte del Estado[117] y se estima que cerca de dos millones de personas han sido encarceladas en "campos de reeducación".[118]

La relación entre el gobierno de Coahuila y dicha empresa parece ser cercana. Entre el 27 y el 31 de mayo del 2018, el gobernador Riquelme realizó una "misión comercial" a China en la que se reunió con la empresa Dahua. Según el informe de dicha gira, Dahua declaró contar con un interés para entrar en el mercado mexicano, "por lo que encuentra en Coahuila a un gran aliado".[119] A finales de octubre del 2019 el gobierno del Estado de Coahuila realizó otra visita a China en la que se "hermanó" a la ciudad de Torreón con la ciudad de Xuzhou.[120] En este viaje se realizaron reuniones de trabajo entre la empresa Dahua, el gobernador Riquelme y presidentes municipales –incluido Manolo Jiménez Salinas, actual gobernador de Coahuila– de algunos de los municipios en los que posteriormente se instaló el sistema de reconocimiento facial, incluyendo Saltillo, Torreón y Monclova.[121] Más adelante, la presentación del Sistema de Video-Inteligencia contó con la presencia del CEO global de Dahua.

El gobierno del estado de Coahuila no ha transparentado las especificaciones de las cámaras de videovigilancia que componen al Sistema de Video Inteligencia. A partir de fotografías de notas periodísticas de las cámaras instaladas, es posible tener una aproximación a las posíbles cámaras que forman parte del sistema. La tabla a continuación muestra los modelos de cámaras y sus especificaciones que podrían ser utilizadas en el sistema de reconocimiento del estado de Coahuila.

//* ----------

116/ Hamilton, Isobel Asher. "Chinese Surveillance Giants Blacklisted by Trump's Administration Are Set to Appear at a Major US Security Trade Show". Business Insider. Accedido 28 de mayo de 2024. https://www.businessinsider.com/blacklisted-surveillance-hikvision-dahua-huawei-security-isc-2020-3

117/ "China's Algorithms of Repression". Human Rights Watch, 1 de mayo de 2019. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

118/ Saucedo, Natalia. "What's Happening In China's Concentration Camps? Q&A with Uyghur Camp Survivors". *Human Rights Foundation* (blog), 13 de abril de 2023. https://hrf.org/whats-happening-in-chinas-concentration-camps-qa-with-uyghur-camp-survivors/

119/ Guerra Pérez, Jaime. Informe General, Visita de Promoción Económica en China del 27 al 31 de mayo de 2019. https://www.coahuilatransparente.gob.mx/RutaDataFiles/otrainfo/documentos_otrainfo/27%20al%2031%20de%20mayo%20China.pdf

120/ Casas, Ilse. "Afianzan relación Coahuila-China", 28 de octubre de 2019. https://www.somosindustria.com/articulo/afianzan-relacion-coahuila-china/

121/ "Gobierno De Coahuila", 5 de diciembre de 2023. https://coahuila.gob.mx/agenda/evento/5d8b8450b3ed87d004000021

TIPO DE CÁMARA ----------//

alhua TECHNOLOGY	NETWORK PTZ
	//MODELOS SD6CE445XA-HNR, SD6CE245U-HNI, SD6CE230U-HNI, SD6CE225U-HNI **//RANGO** 200 m, 250 m **//RESOLUCIÓN** - 1920x 1080 - 2560 x 1440

<ESPECIFICACIONES>
Capacidad de vigilancia de hasta 250 metros en áreas con condiciones diversas de iluminación. Para uso en interior y exterior, en condiciones de temperaturas extremas (40°C - 70°C).

Capaciad de reconocimiento de rostro, objetos presentes o ausentes y perímetro.

TIPO DE CÁMARA ----------//

alhua TECHNOLOGY	PEOPLE COUNTING	PERIMETER PROTECTION	ULTRA-SMART SERIES	ACCESS ANPR
	//MODELOS IPC-HFW8241E-Z IPC-HFW8241E-Z IPC-HFW3241E-Z **//RANGO** 50 m **//RESOLUCIÓN** - 1920 x 1080	**//MODELO** IPC-HFW3241E-Z5 **//RANGO** 100 m **//RESOLUCIÓN** - 1920 x 1080	**//MODELOS** IPC-HFW8232E-ZE IPC-HFW8231E-ZE IPC-HFW8331E-ZE IPC-HFW81230E-Z IPC-HFW8231E-Z5E **//RANGO** 50 m, 100 m **//RESOLUCIÓN** - 1920 x 1080 - 2048 x 1536 - 4000 x 3000	**//MODELO** ITC237-PW1B-IRZ **RANGO** 8 m **//RESOLUCIÓN** - 1920 x 1080

<ESPECIFICACIONES>
Capacidad de vigilancia de hasta 250 metros en áreas con condiciones diversas de iluminación. Para uso en interior y exterior, en condiciones de temperaturas extremas (40°C - 70°C).

Capaciad de reconocimiento de rostro, objetos presentes o ausentes y perímetro.

TIPO DE CÁMARA ----------//

dahua TECHNOLOGY	AI PTZ

	//MODELOS
	SD5A445XA-HNR
	
	//RANGO
	150 m
	
	//RESOLUCIÓN
	- 2560 x 1440

<ESPECIFICACIONES> Reconocimiento de perímetro	

Tiempo después, en el contexto de la pandemia de COVID-19, la empresa donó una cámara con TRF y medición térmica al municipio de Monclova. En la presentación de esta donación, el gobernador Riquelme agradeció de manera pública a Dahua por el "gesto inesperado" y anunció que el estado compraría más cámaras de este tipo en los siguientes días, "necesarios para los médicos en la línea de batalla". Por su parte, el CEO de Dahua Technology México declaró en dicha ocasión que la empresa se encontraba muy feliz de poder colaborar de nuevo con el gobierno de la entidad, quien "ha confiado en nuestra tecnología para implementar equipos de Dahua y fortalecer la estrategia de 'Ciudad Segura' y brindar protección a la población".[122]

Dahua también ha estado presente en los procesos de pruebas y promoción de dicho sistema.[123] En un video promocional del "Sistema de Video Inteligencia para la Seguridad" aparecen rostros de fenotipo asiático siendo identificados, así como videos del proceso de instalación de un sistema de vigilancia por parte de lo que parecen ser miembros de la empresa china Dahua.

En una entrevista, el encargado del C5 habló de la expresión de miembros de Dahua sobre la necesidad de "tropicalizar" el algoritmo de identificación de reconocimiento facial mediante su entrenamiento con el "fenotipo mexicano".[124] Dicha "tropicalización" levanta dudas sobre el acceso a la información que la empresa está teniendo. De manera contradictoria, en respuesta a una solicitud de acceso realizada por R3D, la Secretaría de Seguridad Pública

//* ----------

122/ BNamericas.com. "BNamericas - Dahua Technology dona a Coahuila cámara térm..." Accedido 28 de mayo de 2024. https://www.bnamericas.com/es/noticias/dahua-technology-dona-a-coahuila-camara-termica-para-colaborar-en-prevencion-y-control-de-covid-19

123/ Video de presentación del Sistema de Video Inteligencia para el estado de Coahuila: https://r3d.mx/wp-content/uploads/Presentacion-del-nuevo-Sistema-de-Videointeligencia.mp4

124/ Pérez Villoro, Federico y Robles, Paloma . Quinto Elemento Lab. "Vigilancia Biométrica: El Tortuoso Camino de Coahuila Hacia El Reconocimiento Facial". Accedido el 28 de mayo de 2024. https://quintoelab.org/project/vigilancia-biometrica-reconocimiento-facial-coahuila

de Coahuila declaró que no se comparte con ninguna empresa datos recabados mediante el sistema.[125]

En otras ocasiones, empresas dedicadas al desarrollo de sistemas de TRF se han beneficiado al tener acceso a datos personales de poblaciones racializadas, los cuales han sido utilizados para entrenar a sus sistemas. Por ejemplo, el gobierno de Zimbabwe llegó a un acuerdo con la empresa china CloudWalk para la utilización de datos de su población para lograr que dichos sistemas sean más precisos al identificar personas con tonos de piel oscuros.[126] Artículos académicos han sugerido que China utiliza países de la mayoría global como "laboratorios" para el desarrollo de tecnologías de inteligencia artificial, como el reconocimiento facial.[127]

Este tipo de colonialismo digital suele estar acompañado de dinámicas en las que el proceso de exportación de tecnología hacia los países de la mayoría global incluye la reproducción de normas y formas de uso de dichas tecnologías.[128] Esto es especialmente preocupante al observar el uso que se le ha dado a los sistemas de reconocimiento facial desarrollados por Dahua en su país de origen.

Un sistema para perseguir manifestantes

> "Es algo con lo que se no va a experimentar, sino que ya funcionó bien en ciudades inteligentes de allá (China)"[129] – Miguel Ángel Riquelme, gobernador de Coahuila, en la presentación del Sistema de Video Inteligencia.

El 27 de septiembre de 2020, una serie de protestas feministas estalló en Coahuila, en respuesta al feminicidio de Alondra Gallegos García en la ciudad de Saltillo. Las manifestaciones exigían, entre otras cosas, la destitución del Fiscal General del Estado, Gerardo Márquez Guevara y la renuncia del gobernador Miguel Ángel Riquelme[130] por la negligencia de las au-

//* ----------

125/ Respuesta a solicitud de acceso a la información 887620 realizada por R3D a la Secretaría de Seguridad Pública de Coahuila. https://r3d.mx/wp-content/uploads/Respuesta-Coahuila-887620.pdf

126/ Chutel, Lyndsey. "China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database". Quartz. 25 de mayo de 2018. https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity

127/ Gravett, Willem. "Digital Coloniser? China and Artificial Intelligence in Africa". Survival 62 (1 de noviembre de 2020): 153-78. https://doi.org/10.1080/00396338.2020.1851098

128/ Browne, Grace. "AI Is Steeped in Big Tech's 'Digital Colonialism'". Wired. Accedido 28 de mayo de 2024. https://www.wired.com/story/abeba-birhane-ai-datasets/

129/ Vanguardia MX. "Adquiere Gobierno Estatal sistema de video-inteligencia para vigilar Coahuila", 2 de abril de 2019. https://vanguardia.com.mx/coahuila/saltillo/adquiere-gobierno-estatal-sistema-de-video-inteligencia-para-vigilar-coahuila-MRVG3450862

130/ Sánchez, Esmeralda. "Coahuila. Exigen justicia para Alondra, joven hallada muerta". Grupo Milenio, 27 de septiembre de 2020. https://www.milenio.com/estados/coahuila-exigen-justicia-alondra-joven-hallada-muerta

toridades para investigar la desaparición de Alondra. Estas protestas fueron monitoreadas por el sistema de videovigilancia recién instalado en el estado, mediante el cual se registraron 44.7 millones de capturas de rostros de las personas asistentes.[131]

Una de las preocupaciones que ha llevado a la prohibición de este tipo de sistemas en otras ciudades del mundo[132] ha sido precisamente el uso que se le puede dar para perseguir y criminalizar asistentes a protestas. Esto ocurrió en Estados Unidos, en donde por lo menos seis autoridades federales, incluyendo el FBI, utilizaron tecnologías de reconocimiento facial –incluso la desarrollada por la controversial empresa Clearview AI– para identificar a personas que se manifestaron en contra de la brutalidad policial ejercida hacia personas afroamericanas en 2020.[133] Esta práctica puso en relieve el uso distópico del reconocimiento facial en contra de la libertad de expresión, asociación y el derecho a la privacidad de las personas que protestaban en contra de severas violaciones por parte de la autoridad.

Precisamente, el Sistema de Video Inteligencia instalado en Coahuila ha sido utilizado de manera similar. Mediante este sistema, se identificó y ubicó el paradero de Mena Yousif y Jose Felan, perseguidos por el FBI y que participaron en las mencionadas protestas por el asesinato del afroamericano George Floyd a manos de la policía. Felan era buscado por haber cometido actos vandálicos en las protestas ocurridas en Minneapolis y Yousif por ayudarle a escapar. Felan y Yousif, quienes son pareja, cruzaron a México desde el estado de Texas ingresando por Coahuila, buscando evadir la persecución policiaca en la que se encontraban.

En una visita a uno de los C4, el investigador periodístico Federico Pérez Villoro vio la fotografía de una mujer que usaba un hiyab; tiempo después se enteró que se trataba de Mena Yousif. El gobierno de Estados Unidos había solicitado a la Secretaría de Seguridad de Coahuila que utilizara el sistema de reconocimiento facial para ubicar a Yousif y Felan, quienes habían sido descritos por el gobierno de Estados Unidos como terroristas.

Un ex agente del FBI, que ahora es miembro del Centro Brennan para la Justicia, declaró que las instituciones de justicia de ese país tenían en la mira casos como estos para convertirlos en emblemáticos, una estrategia apuntada a criminalizar las protestas contra el asesinato de Floyd.[134] De acuerdo a una nota del medio *New York Times*, el gobierno de Estados Unidos evitó manifestarse sobre los cuestionamientos relativos a

//* ----------

131/ Pérez Villoro, Federico y Robles, Paloma . Quinto Elemento Lab. "Vigilancia Biométrica: El Tortuoso Camino de Coahuila Hacia El Reconocimiento Facial". Accedido 28 de mayo de 2024. https://quintoelab.org/project/vigilancia-biometrica-reconocimiento-facial-coahuila

132/ Schwartz, Nathan Sheard and Adam. "The Movement to Ban Government Use of Face Recognition". Electronic Frontier Foundation, 5 de mayo de 2022. https://www.eff.org/nb/deeplinks/2022/05/movement-ban-government-use-face-recognition

133/ Leon, Radhamely De. "Six Federal Agencies Used Facial Recognition On George Floyd Protestors". Vice (blog), 30 de junio de 2021. https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors

134/ Hill, Kashmir. "A Fire in Minnesota. An Arrest in Mexico. Cameras Everywhere." The New York Times, 1 de agosto de 2021, sec. Technology. https://www.nytimes.com/2021/08/01/technology/minneapolis-protests-facial-recognition.html

su solicitud en el uso de un sistema de vigilancia del estado de Coahuila para la persecución de Felan y Yusif.[135]

RECONOCIMIENTO FACIAL EN AGUASCALIENTES

MUNICIPIO DE AGUASCALIENTES: VIDEOVIGILANCIA URBANA INTEGRAL CON TECNOLOGÍA ANALÍTICA

En 2018, durante el gobierno de María Teresa Jiménez Esquivel (conocida públicamente como Tere Jiménez), el municipio de Aguascalientes adquirió sistemas de vigilancia para el proyecto de "Videovigilancia Urbana Integral con Tecnología Analítica", el cual incluyó la instalación de 200 cámaras de videovigilancia, de las cuales, 30 puntos cuentan con capacidades de reconocimiento facial y de identificación de matrículas.[136]

El proyecto tuvo un costo total de 53 millones de pesos, financiado con recursos de del FORTASEG –un subsidio federal para el fortalecimiento de la seguridad otorgado a estados y municipios– por 14 millones de pesos mediante el contrato PS 048/2018,[137] así como también a través de recursos del mismo municipio por 39 millones de pesos.[138]

El sistema fue inaugurado el 1 de enero de 2019 y es operado por el Centro de Comando, Control, Comunicación y Cómputo (C4), dependencia de la Secretaría de Seguridad Pública a nivel municipal. De acuerdo al tercer informe de trabajo 2017 - 2019 de la administración de Tere Jiménez, a finales del año 2019, mediante el proyecto de Videovigilancia Urbana Integral con Tecnología Analítica se pusieron en operación tres Centros de Control (C2) en las localidades de Pocitos, Jesús Terán e Insurgentes. Además, se integraron sistemas de videovigilancia privados de empresas, negocios y hogares al sistema de vigilancia del gobierno.[139]

La información pública disponible sobre la forma en que se utiliza el sistema de TRF –referente al número de personas que han sido detenidas a partir de su uso– se limita a un comunicado del ayuntamiento de Aguascalientes publicado en el año 2019, que relata la supuesta aprehensión de una persona por tentativa de robo, detectada mediante el uso de

//* ----------

135/ Hill, Kashmir. "A Fire in Minnesota. An Arrest in Mexico. Cameras Everywhere." The New York Times, 1 de agosto de 2021, sec. Technology. https://www.nytimes.com/2021/08/01/technology/minneapolis-protests-facial-recognition.html

136/ Auditoría Superior de la Federación. "Auditoría De Cumplimiento: 2018-D-01001-19-0537-2019". 2019. pg. 9. https://www.asf.gob.mx/Trans/Informes/IR2018c/Documentos/Auditorias/2018_0537_a.pdf

137/ Respuesta a solicitud de acceso a la información 0100536224000364 realizada por R3D a la Secretaría de Administración del municipio de Aguascalientes. https://r3d.mx/wp-content/uploads/RESP-AD-364-2024.pdf

138/ Desde la Red. "120% más cámaras de videovigilancia habrá en el Municipio de Aguascalientes". Accedido 14 de agosto de 2024. https://www.desdelared.com.mx/noticias/2019/01-municipio/0131-120-por-ciento-mas-camaras-de-videovigilancia-habra-en-el-municipio-de-aguascalientes.html

139/ "Tercer Informe Tere Jiménez, Aguascalientes. Lo Mejor Está Por Venir.", 13 de septiembre de 2019. Municipio de Aguascalientes. https://issuu.com/stratomarketing/docs/aytoags-3inf_30ago-1100-multicolor_portada_issuu. pg.25.

dicho sistema.[140] La posición oficial argumenta que dicho sistema ayudó a reducir la percepción de inseguridad en 8.7 puntos porcentuales.

El sistema de TRF utilizado fue integrado por la empresa mexicana "Compañía Integra Soluciones S.A. de C.V.", también conocida como Integra Technologies. Según el director de dicha empresa, el sistema incluye la instalación de cámaras de videovigilancia de la empresa estatal china Hikvision.[141]

En 2021, la empresa Integra ganó el concurso por licitación GMA-017-C-2021 por la "Adquisición y Servicio de Instalación de Kits De Cámaras de Vigilancia Requerido por la Secretaría de Seguridad Pública".[142] Mediante el contrato AD 039/2021 por la cantidad de un millón 199 mil 904 pesos, el municipio de Aguascalientes adquirió dentro de esta licitación 400 cámaras adicionales de la marca UNV o DAHUA, así como almacenamiento por 2.5 terabytes, y el servicio de la incorporación de cámaras del sector privado y casa habitación al sistema municipal de videovigilancia, incrementando las capacidades de vigilancia del sistema.[143]

ESTADO DE AGUASCALIENTES: C5 SITEC

En 2018, el gobierno estatal de Aguascalientes –bajo el mando del gobernador Martín Orozco Sandoval– celebró un contrato plurianual para la implementación del Centro de Comando, Control, Comunicación, Cómputo y Coordinación "C5 SITEC", el cual incluyó la adquisición de servicios y equipamiento de videovigilancia con capacidades de reconocimiento facial entre los años 2018 y 2022 con un costo total de 728 millones 10 mil 176 pesos.[144]

El contrato 205/2018 de adjudicación directa fue otorgado a la empresa SYM Servicios Integrales, S.A. de C.V. En los últimos años, esta empresa ha sido intermediaria en la venta de diversos sistemas de vigilancia, entre los que se encuentra el malware Galileo –desarrollado por la empresa italiana Hacking Team–, vendido en 2013 al gobierno de Rafael Moreno Valle en el estado de Puebla para vigilar a opositores políticos.[145] Otros clientes de esta empresa

//* ----------

140/ Municipio de Aguascalientes. "Nuevas cámaras de seguridad arrojan resultados positivos". 30 de enero de 2019. https://www.ags.gob.mx/cont.aspx?p=6253

141/ inst:all. "Hikvision e Integra Technologies entregan una solución de vigilancia ciudadana al municipio de Aguascalientes". Inst:all magazine, 27 de octubre de 2020. https://installmagazine.com.mx/hikvision-e-integra-technologies-entregan-una-solucion-de-vigilancia-ciudadana-al-municipio-de-aguascalientes/

142/ Fallo del concurso por licitación para la adquisición y servicio de instalación de kits de cámaras de vigilancia requerido por la Secretaría de Seguridad Pública de Aguascalientes. https://r3d.mx/wp-content/uploads/FALLO-DE-ADJ-GMA-017-C-2021.pdf

143/ Respuesta a solicitud de acceso a la información 0100536224000370 realizada por R3D a la Secretaría de Administración del municipio de Aguascalientes. https://r3d.mx/wp-content/uploads/2024-Escaneo-3.pdf

144/ Contrato plurianual de solución tecnológica para la implementación integral del Centro de Comandando, Control, Comunicación, Cómputo y Coordinación "C5 SITEC". https://r3d.mx/wp-content/uploads/205_2018.pdf

145/ Digitales, R3D: Red en Defensa de los Derechos. "NYT documenta uso de malware para espionaje político en Puebla". R3D: Red en Defensa de los Derechos Digitales (blog), 5 de enero de 2017. https://r3d.mx/2017/01/05/nyt-documenta-uso-de-malware-para-espionaje-politico-en-puebla/

en México que adquirieron sistemas de malware desarrollados por Hacking Team son los gobiernos estatales de Campeche[146] y Jalisco.[147] SYM Servicios Integrales, S.A. de C.V. también es filial del grupo Kabat, empresa de origen Israelí que incluye entre sus asesores a exmilitares del ejército mexicano.[148]

La versión pública del contrato, obtenida por R3D mediante una solicitud de acceso a la información, no transparenta los componentes que conforman al sistema de TRF adquirido por el gobierno del estado de Aguascalientes. Sin embargo, un documento entregado por SYM Servicios Integrales dentro del proceso de venta, relativo a la exclusividad de venta para comercializar productos de la empresa israelí CityShob Software Development LTD, revela que el C5 SITEC cuenta con un plataforma central llamado CityMIND.[149]

De acuerdo a una nota periodística, hasta el año 2019, la instalación del equipamiento tecnológico del sistema de videovigilancia con TRF correspondiente al contrato 205/2018 se encontraba concluida apenas en un dos por ciento.[150] A través del cumplimiento a la resolución de recurso de revisión con el número de folio 0112/2021[151] se ha logrado conocer que no se han realizado estudios de impacto del sistema en los derechos de la población ni auditorías externas sobre el funcionamiento del sistema. Las personas identificadas mediante el uso del sistema tampoco son notificadas. Según la respuesta del C5 SITEC en dicho cumplimiento, el sistema comenzó a ser utilizado en el mes de noviembre de 2020.

A partir del cumplimiento a un recurso de inconformidad –correspondiente al recurso de revisión antes mencionado– ha sido posible conocer, de manera limitada, la forma en que la Secretaría de Seguridad Pública del Estado de Aguascalientes está utilizando el sistema de reconocimiento facial.[152]

//* ----------

146/ Niv M. Yarimi. "FW: END USER HT.pdf". WikiLeaks - The Hacking Team Archives. Accedido 14 de agosto de 2024. https://wikileaks.org/hackingteam/emails/emailid/4285

147/ Serge Woon. "Re: Ticket SDUC" WikiLeaks - The Hacking Team Archives. Accedido 14 de agosto de 2024. https://wikileaks.org/hackingteam/emails/emailid/667505 y Santana, R. "Niegan Campeche y Yucatán compra de software para espiar a ciudadanos". Proceso. 7 de julio de 2015. http://www.proceso.com.mx/409980/niegan-campeche-y-yucatan-compra-de-software-para-espiar-a-ciudadanos

148/ Paginabierta. "Ex militares mexicanos asesoran a empresa que vendió software de espionaje", 11 de julio de 2015. https://paginabierta.mx/2015/07/11/ex-militares-mexicanos-asesoran-a-empresa-que-vendio-software-de-espionaje/

149/ Acuerdo de exclusividad emitido por la empresa CityShob para la empresa SYM Servicios Integrales, S.A. de C.V. https://r3d.mx/wp-content/uploads/carta_exclusividad_cityshob.pdf, pg. 434.

150/ Revista Construye. "Continúan con infraestructura de seguridad publica". Revista Construye (blog), 3 de enero de 2020. https://revistaconstruye.com.mx/continuan-con-infraestructura-de-seguridad-publica/

151/ Cumplimiento a la resolución RR 0112/2021, solicitud 00095321 realizada a la Secretaría de Seguridad Pública del Estado de Aguascalientes. https://r3d.mx/wp-content/uploads/CUMPLIMIENTO-RESOLUCION-112-2021-13-10-21.pdf

152/ Cumplimiento a la resolución RR 0112/2021, solicitud 00095321 realizada a la Secretaría de Seguridad Pública del Estado de Aguascalientes. https://r3d.mx/wp-content/uploads/CUMPLIMIENTO-RESOLUCION-112-2021-13-10-21.pdf

La autoridad respondió que, hasta octubre de 2021, la base de datos utilizada para el reconocimiento de personas contaba con 119 registros. Las categorías de datos que contiene dicha base de datos incluyen: nombre, fecha de nacimiento, fotografía e identificación del requerimiento. En dicho cumplimiento, la autoridad indica que la empresa proveedora tiene acceso indirecto a los sistemas, debido a que es la encargada de ofrecer mantenimiento correctivo. Al respecto, la secretaría fue explícita en determinar que no se genera documentación al respecto y que el C5 puede proveer acceso al equipo o sistema de manera remota. Por otra parte, agentes de la Fiscalía General del Estado de Aguascalientes, policía municipal y estatal, Protección Civil y Servicios Médicos son algunas de las autoridades que tienen acceso al uso del sistema.

Por último, la SSP determina que las normativas que regulan las atribuciones para la utilización el sistema de vigilancia con capacidad de reconocimiento facial son: la Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video-Vigilancia para la Seguridad Pública y la Ley de Videovigilancia del Estado de Aguascalientes.

La Norma Técnica sobre videovigilancia no es un fundamento aplicable para las cámaras con TRF porque está pensada para videovigilancia tradicional. Esta norma está desactualizada, pues fue emitida en 2016 y se basa en fundamentos jurídicos no aplicables para México que datan de hace más de una década.

Aplicar este estándar concebido para videovigilancia convencional al contexto de TRF puede aumentar el riesgo de abusos, ya que parte de la premisa de que todas las personas son sospechosas y es necesario vigilarlas. En ese sentido, establece la necesidad de colocar un mayor número de cámaras en zonas socialmente rezagadas, lo cual puede impactar negativamente a grupos en situación de vulnerabilidad, como personas en condiciones de pobreza.

Además, no provee estándares para medir la eficiencia y efectividad en la operación de las infraestructuras de videovigilancia. Únicamente establece parámetros sobre su instalación, los cuales pueden diferir mucho entre un sistema de videovigilancia tradicional y uno con TRF. Por ejemplo, esta norma provee información sobre el ángulo de la cámara o la iluminación. Sin embargo, los sistemas tradicionales tienen capacidades distintas a los de TRF y no es adecuado utilizar los mismos parámetros. Por tanto, no es un fundamento aplicable ni adecuado para la implementación de este sistema.

La Ley de Videovigilancia del Estado de Aguascalientes regula el uso de tecnologías de videovigilancia. No obstante, no existe una disposición en específico en esta ley que regule el uso de TRF. En su artículo tercero define la videovigilancia de la siguiente forma:

> La captación de imágenes con o sin sonido en lugares públicos o privados con acceso al público, por los cuerpos de seguridad pública estatal o municipales o de seguridad privada, para la investigación de delitos y la documentación de faltas administrativas relacionadas con la seguridad pública, que realicen en términos de la presente Ley.

Este concepto abarca el uso de cámaras en el espacio público pero no menciona el uso de TRF. Aunque la TRF sí utiliza las imágenes que se recaban por las cámaras, el procesamiento de estas imágenes para obtener los marcos faciales e identificar a la persona es distinto y sumamente invasivo. Aguascalientes debió haber tenido una legislación que incluye de manera clara y precisa el uso de TRF previo a su implementación en el espacio público.

Actualización del sistema estatal en el año 2022

En el año 2022, el gobierno del estado de Aguascalientes adquirió bienes y servicios adicionales para el C5 SITEC mediante el contrato de adjudicación directa número 092/2022-DIRECTA-SSP,otorgado una vez más a la empresa SYM Servicios Integrales.[153]

Dicho contrato, por la cantidad de 50 millones 995 mil 444 pesos incluyó la adquisición de sistemas de vigilancia adicionales a los comprados en 2018. Por ejemplo, la descripción de los bienes y servicios adquiridos contiene un apartado para la adquisición de un sistema de videovigilancia a ser instalado en el parque público Bordo Santa Elena. Entre las obligaciones del proveedor incluidas en el contrato se menciona que los bienes y servicios adquiridos deberán ser 100 por ciento compatibles con la Plataforma Central CityMIND.[154]

La convocatoria DGAD-IE-03-2023 para el servicio de mantenimiento a la plataforma del C5 SITEC (C5i) para los años 2023 al 2025, publicada en el año 2023 por el gobierno del Estado de Aguascalientes –ya bajo la administración estatal de Tere Jimenez– revela parte de los componentes del sistema de vigilancia con TRF adquiridas por dicho gobierno en los años 2019 y 2022.[155] Dicha convocatoria menciona algunos de los componentes que conforman la Plataforma Central CityMIND del C5i, como se muestra en la tabla a continuación.

//* ----------

153/ Contrato para la adquisición de bienes y prestación de servicios de la solución integral para nuevas capacidades y cobertura de la red de la dirección general del centro estatal de telecomunicaciones C-4, operando bajo la denominación: Centro de Comando, Control, Comunicación, Cómputo y Coordinación "C5 SITEC" y del sitio alterno (C4 estatal) y nuevos puntos de monitoreo en instalaciones y ubicaciones estratégicas. https://r3d.mx/wp-content/uploads/092-22.pdf

154/ *Ibid*. pg.6.

155/ Convocatoria de la invitación a cuando menos tres personas por excepción número DGAD-IE-03-2023 de la Secretaría de Administración del Estado de Aguascalientes. https://r3d.mx/wp-content/uploads/DGAD-IE-03-23-C.pdf

//SISTEMA	//DESARROLLADOR	//----- DESCRIPCIÓN -----//	//NÚMERO DE LICENCIAS
C-INSIGHT	CITYSHOB SOFTWARE DEVELOPMENT LTD	Plataforma integradora con capacidad para agregar y analizar datos provenientes de fuentes como sensores, cámaras, mapas, redes sociales y fuentes abiertas. Cuenta con las siguientes capacidades: (1)Análisis para el rastreo de vehículos, personas, reconocimiento de rostros y la ubicación de estos eventos en el espacio, así como la identificación de patrones y tendencias. (2) Detección automática y alerta de incidentes. (3) Monitoreo en redes sociales.	108
C-REACT	CITYSHOB SOFTWARE DEVELOPMENT LTD	Aplicación de dispositivos móviles (tabletas) para el uso de agentes de campo. Dicha aplicación permite a los agentes en campo tener acceso a información del C5i en tiempo real. No es posible conocer a partir de la información pública a qué tipo de información del C5i se puede tener acceso.	100
SISTEMA VMS FLIR LATITUDE	TELEDYNE TECHNOLOGIES INCORPORATED	Sistema de vigilancia IP cuenta con generación de imágenes de calidad forense. La arquitectura escalable admite implementar sistemas que abarquen ciudades enteras. La aplicación permite acceso al estado del sistema y video de manera remota en cualquier momento y lugar.	2930
NEUROCAR V 4.4.1	NEUROCAR SP. Z O. O.	Aplicación diseñada para detección e identificación de números de placa de vehículos en movimiento.	224
OOSTO V2	ANYVISION INTERACTIVE TECHNOLOGIES LTD.	No hay información pública disponible para conocer específicamente cuál es el producto utilizado entre los desarrollados por Oosto. El sitio de la empresa contiene dos soluciones que cuentan con capacidades de reconocimiento facial, para identificar rostros, poses y comportamiento (caídas, movimiento), así como vivacidad. Los productos que la empresa ofrece pueden ser utilizados en dispositivos móviles -incluidos teléfonos móviles o cámaras corporales- y en sistemas de videovigilancia fijos. La identificación de rostros se realiza en tiempo real a partir de listas de interés o a partir del análisis de material de video anteriormente capturado.	25

La empresa CityShob menciona al proyecto de videovigilancia del estado de Aguascalientes en su sitio web.[156] Según la empresa, el sistema instalado permite la operación de más de 100 agentes, la incorporación de 10 centros locales de Comando y Control (C2), la integración de sistemas VMS que operan más de tres mil cámaras, de las cuales 220 cámaras están dedicadas a la identificación automática de matrículas. También se menciona la integración del sistema de vigilancia del transporte público.

La convocatoria DGAD-IE-03-2023 también buscó la ampliación y actualización de varios de los sistemas anteriormente mencionados. Dicha petición incluye la implementación de una nueva interfaz con compatibilidad con el sistema operativo Android, que "convierte" a los teléfonos celulares de los agentes en campo en una extensión de C-React y C-Insight. Este también hace posible la interacción entre el operador en campo y el del C5 mediante el chat nativo de C-React. De nuevo, no hay mucha más información pública disponible para conocer exáctamente como funciona dicha interacción.

//---------- CÁMARAS ----------//

//FOTOGRAFÍA	//MODELO	//EMPRESA	// TIPO DE CÁMARA	//ESPECIFICACIONES	//RESOLUCIÓN	//NÚMERO DE CÁMARAS
	CM-3102-11-I Y/O CM-3202-11-I (FLIR)	Teledyne Technologies Incorporated	FIJA	Capacidad de vigilancia de hasta 30 m, utilizable en ambientes con poca luz.	1920 X 1080	1519
	CP-6302-31-I (FLIR)	Teledyne Technologies Incorporated	PTZ	Capacidad de vigilancia de hasta 200 metros en áreas con condiciones diversas de iluminación. Para uso en interior y exterior, tanto de día como de noche. Zoom óptico digital 30x /hasta 10X	1920 X 1080	611
	CF-5222 (FLIR)	Teledyne Technologies Incorporated	ANALÍTICA	Visión nocturna y en lugares con poca iluminación. Según la página de la empresa fabricante este modelo de cámara fue descontinuada.	1280 X 1024	500

//* ----------

156/ CityShob. "Aguascalientes". Accedido 14 de agosto de 2024. https://cityshob.com/es/projects-2/aguascalientes/

Mediante la convocatoria previamente mencionada, el gobierno del estado de Aguascalientes buscó actualizar el sistema de reconocimiento facial instalado en la entidad para permitir que las cámaras que cuenten con la licencia de reconocimiento facial "constituyan un sistema de seguridad proactivo". Esto implica la generación de alertas automáticas a través del uso del programa C-Insight en caso de (1) coincidencia de personas con características específicas y (2) coincidencia de personas que formen parte de las listas de personas buscadas.

Además, la convocatoria también solicitó una configuración para la reasignación de licencias existentes en diversas cámaras, lo que abre la posibilidad de hacer uso de TRF en todas las cámaras del sistema. Por otro lado, la convocatoria de ampliación también solicitó "mantener eficiencia en lecturas del 90% en el reconocimiento de rostros", lo que levanta dudas sobre la eficiencia del sistema hasta ese momento. Esta convocatoria fue ganada por la empresa Blindajes Urbanos, S.A. de C.V. por la cantidad de 129 millones 289 mil 272 pesos.[157]

Uso del reconocimiento facial en contexto de protesta

Las TRF son especialmente peligrosas para la libertad de expresión cuando se usan para vigilar las protestas públicas. El 8 de marzo de 2021, distintas activistas feministas se congregaron en el centro de la ciudad para manifestarse. Lamentablemente, se ha documentado que fueron intimidadas por elementos de la seguridad pública del estado. Los elementos de policía identificaron a integrantes de la marcha por nombre y apellido, a pesar de no haber hecho ninguna referencia a esto en ninguna de sus redes digitales.[158]

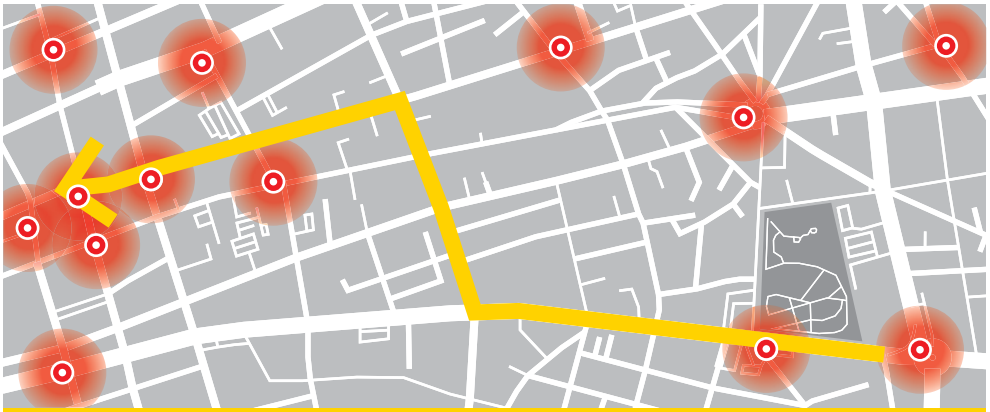
Una de las activistas involucradas expresó su preocupación por ser objeto de vigilancia al indicar que "hubo represión policial, quiero meter una solicitud de cancelación de datos personales porque no sé cómo obtuvieron mi información". Posteriormente, se identificó que se han instalado cámaras con TRF a lo largo de la ruta de la marcha del 8 de marzo de 2024.

En general, esta ruta ha sido utilizada por distintos movimientos para ejercer su derecho a la protesta. La instalación de dichas cámaras supone una obstrucción para que las personas puedan manifestarse de manera libre y sin temor a represalias.

//* ----------

157/ Acta de emisión de fallo y de notificación de la convocatoria de la invitación a cuando menos tres personas por excepción número DGAD-IE-03-2023-F de la Secretaría de Administración del Estado de Aguascalientes. https://r3d.mx/wp-content/uploads/DGAD-IE-03-23-F.pdf

158/ Loucaides, Darren. "The changing face of protest". Rest of world. 27 de Marzo de 2024. Accedido por última vez el 20 de agosto de 2024 en: https://restofworld.org/2024/facial-recognition-government-protest-surveillance/



< Ruta de la marcha 8m 2024 y ubicación de cámaras />

Distintos gobiernos justifican el uso indiscriminado de TRF en contextos de protesta bajo el argumento de garantizar la seguridad pública. No obstante, existe una multiplicidad de casos en los que las autoridades estatales abusan de estas herramientas para inhibir protestas y perseguir legalmente a manifestantes que ejercen sus derechos. En Rusia han utilizado esta tecnología para perseguir criminalmente a manifestantes que se oponen al gobierno. El gobierno ruso utilizó TRF para identificar y detener a personas que iban a asistir a las protestas en contra de la guerra en Ucrania.[159] En India se utilizaron conjuntos de datos biométricos sobre manifestantes habituales, los cuales se integraron a las TRF que monitorean grandes multitudes. Estas bases de datos fueron empleadas para identificar a opositores políticos y detenerlos.

Durante las protestas de Hong Kong en 2019, los manifestantes usaron paraguas para cubrir su rostro y evitar la identificación de las cámaras de TRF.[160] Anteriormente, dichas cámaras habían sido utilizadas por la policía para identificar a los manifestantes y monitorear sus movimientos.[161] El fin de esta vigilancia con TRF es impedir cualquier tipo de manifestación contra el gobierno. Inclusive, se ha documentado su utilización para la opresión sistemática de grupos étnicos y religiosos, por ejemplo, en la región de Xinjiang en China.[163]

Cuando no existe una expectativa de privacidad en espacio públicos, las personas moderan sus conductas. La vigilancia masiva e indiscriminada inhibe a las personas a expresarse libremente. Esto abarca desde poder realizar nuestra vida cotidiana con tranquilidad hasta asistir a protestas públicas.

//* ----------

159/ *Idem*.

160/ *Idem*.

161/ Zalnieriute, Mónica. “Power and Protest: Facial Recognition and Public Space Surveillance”. The Cambridge Handbook of Facial Recognition In the Modern State. Cambridge University Press. 2024.

162/ Mozur, Paul.“In Hong Kong Protests, Faces Become Weapons” New York Times. 26 de julio 2019.

163/ Redacción. “HRW: Reconocimiento Facial y Análisis Datos, Al Servicio De China En Xinjiang.” La Vanguardia, 2 May 2019 Consulta en: www.lavanguardia.com/politica/20190502/461994950390/hrw-reconocimiento-facial-y-analisis-datos-al-servicio-de-china-en-xinjiang.html

El anonimato constituye un medio para la protección de la privacidad y ha sido particularmente destacado en su relación con la libertad de expresión por facilitar la participación en el discurso público sin identificarse, evitando de esta manera posibles represalias asociadas con la opinión. Por ello, deben garantizarse espacios anónimos, libres de observación y documentación de actividades e identidades.[164] A pesar de esto, la implementación de TRF en ciudades obstaculiza gravemente la posibilidad a asistir a una manifestación de manera anónima.

BLINDAJE AGUASCALIENTES: OTRAS INICIATIVAS ESTATALES DE RECONOCIMIENTO FACIAL

La introducción de sistemas de reconocimiento facial y de lectura de matrículas vehiculares durante la administración estatal de Tere Jimenez es parte de su plan de seguridad llamado "Blindaje Aguascalientes", el cual incluye –además de la ampliación de las capacidades del C5i– otros proyectos relacionados al uso de TRF.

Uno de estos es el titulado "Puertas de Acceso" el cual se conforma por la construcción de sitios de revisión ubicados en cinco puntos limítrofes del estado de Aguascalientes sobre autopistas en la zona norte, sur, oriente por la salida a San Luis Potosí, Asientos y Calvillo. Dicho proyecto tuvo un costo de 22.5 millones de pesos, según el titular de la Secretaría de Seguridad Pública del Estado, Manuel Alonso García.[165]

Otros dos proyectos de este tipo que comprenden las torres de vigilancia móviles conocidas como Sketchwatch[166] y la unidad móvil, las cuales cuentan con TRF y lectura de matrículas. Según Alonso García, dichas torres están diseñadas para funcionar en áreas sin cobertura a Internet. La unidad móvil es un vehículo de remolque Ford modelo Super Duty –conectado al C5i– equipado con cámaras de reconocimiento facial, visión 360 grados y una sala de crisis.

El titular de la Secretaría de Seguridad Pública ha declarado que el vehículo será utilizado en zonas de difícil acceso, eventos multitudinarios y operativos especiales. Esta unidad tuvo un costo de 10 millones de pesos.[167]

Por último, se encuentra la adquisición de mil cámaras corporales por parte del gobierno de Aguascalientes, sobre las cuales no existe información que detalle si están siendo utilizadas con TRF, pero podría ser una posibilidad, dadas las capacidades de los demás sistemas de vigilancia en el espacio público con los que cuenta el estado.

//* ----------

164/ CIDH. Libertad de Expresión e Internet. Párr. 130-134.

165/ Giovanni Góngora. "Entregan Puerta de Acceso en Asientos". El Sol del Centro. Accedido 14 de agosto de 2024. https://www.elsoldelcentro.com.mx/local/entregan-puerta-de-acceso-en-asientos-10695229.html

166/ Cecilia De Santos Velasco "Llegan ascensos, torres de vigilancia y cámaras corporales a la Policía de Aguascalientes" El Heraldo de Aguascalientes. Accedido 14 de agosto de 2024. https://www.heraldo.mx/llegan-ascensos-torres-de-vigilancia-y-camaras-corporales-a-la-policia-de-aguascalientes

167/ Rubén Torres. "Aumenta la vigilancia con el "C2 Móvil"". El Sol del Centro . Accedido 14 de agosto de 2024. https://oem.com.mx/elsoldelcentro/local/aumenta-la-vigilancia-con-el-c2-movil-14407440

CAP.03\\

UNA SOLUCIÓN EN BÚSQUEDA DE UN PROBLEMA: LA IMPLEMENTACIÓN DE TRF EN AEROPUERTOS.

Las personas usan constantemente los aeropuertos para conectarse con otras partes de su país o del mundo. En promedio, hay 100 mil traslados aéreos por día globalmente. El tránsito dentro de los aeropuertos es caótico en distintas escalas. En estos espacios vemos desde familias corriendo para alcanzar sus vuelos hasta personas detenidas arbitrariamente por parte de las autoridades migratorias.

La instalación de TRF en aeropuertos pone en riesgo los derechos de sus usuarios e incrementa el caos en las terminales. Los proveedores de TRF y sistemas de procesamiento de pasajeros promueven esta tecnología como una forma de hacer más sencillo el proceso, sin embargo, lo que realmente ofrecen es un servicio que promueve la vigilancia masiva y ponen en riesgo a grupos históricamente discriminados. Los gobiernos que promueven la TRF en aeropuertos nos piden, básicamente, que entreguemos nuestras libertades a cambio de esperar menos tiempo en las filas.

+ LA TRF EN LOS AEROPUERTOS DEL MUNDO

El atentado del 11 de septiembre de 2001 cambió de forma radical las políticas de seguridad en los aeropuertos. La implementación de las políticas de vigilancia masiva en los aeropuertos son un resultado de la implementación de legislación como la *Patriot Act*. Parte de esta política incluyó el uso de tecnología biométrica para facilitar la identificación de las personas extranjeras, con el fin de facilitar las operaciones de seguridad y prevenir ataques terroristas.[168]

En Estados Unidos, se instalaron una serie de escáneres de rostro en distintos aeropuertos.[169] En principio, todas las personas pasajeras de vuelos internacionales deben registrar sus rostros en estos escáneres que utilizan una base de datos biométricos administrada por el Departamento de Seguridad Nacional (DHS, en adelante, por sus siglas en inglés).

La implementación de este sistema ha sido criticada por personas expertas y organizaciones defensoras de derechos humanos. El *Center on Privacy and Technology* describió estos escáneres como una "solución en búsqueda de un problema". El DHS manifestó que los prin-

//* ----------

168/ Radison Rudolph, Laura Moy M., y Bedoya, Alvaro M., "Not Ready for Takeoff", Georgetown Law Center on Privacy & Technology. 21 de Octubre de 2017. Consultado el 15 de julio de 2024 en: https://www.airportfacescans.com/sites/default/files/Biometrics_Report__Not_Ready_For_Takeoff.pdf

169/ *Id.*

cipales objetivos de este sistema son, primero, evitar que una persona terrorista se identifique con credenciales falsas y entre al país; el segundo objetivo busca que estos escáneres eviten el fraude de visas de turistas.

El DHS no ha logrado justificar cómo estos escáneres contribuyen a lograr ese objetivo, a pesar de haber invertido un aproximado de mil millones de dólares en este sistema. Incluso, el mismo DHS señaló que quedaban dudas sobre el valor adicional que una puerta biométrica pueda proveer en comparación con los sistemas actuales que no usan TRF.

De igual forma, distintas organizaciones de sociedad civil y la academia manifestaron su preocupación debido a que los escáneres faciales representan un grave riesgo para la privacidad de las personas. El DHS comenzó la implementación de este sistema con la pretensión de que fuera obligatorio para todas las personas pasajeras. Posteriormente, el DHS revirtió esa decisión después de enfrentar severas críticas por parte de ONGs y activistas.

Sin embargo, las problemáticas que ponen en riesgo la privacidad persisten. El sistema de procesamiento de pasajeros busca la interoperabilidad con otras bases de datos policiacas y compartir información con otras agencias gubernamentales de manera arbitraria. De igual forma, es preocupante que la infraestructura necesaria para implementar esta TRF es provista por las mismas aerolíneas. La DHS no ha auditado a la mayoría de las aerolíneas con quienes comparten la información biométrica de los pasajeros.[170] La Unión Americana de Libertades Civiles (ACLU, por sus siglas en inglés) manifestó que este tipo de medidas resulta en que las aerolíneas generen perfiles biométricos de los pasajeros de manera masiva y sin ningún tipo de control.[171]

LA TRF EN EL AEROPUERTO INTERNACIONAL FELIPE ÁNGELES

El 20 de diciembre de 2018, el entonces presidente Andrés Manuel López Obrador anunció que la construcción del Aeropuerto Internacional Felipe Ángeles (AIFA) estaría en manos de la Secretaría de Defensa Nacional (SEDENA), encargada del ejército y las fuerzas armadas en México.

En abril de 2019, antes de que iniciaran las obras, la SEDENA asumió el control total del proyecto. Poco tiempo después, el Consejo de Seguridad Nacional declaró que lo relacionado con el AIFA debía ser considerado como un asunto de seguridad nacional, lo cual habilita la opacidad de la información relacionada con el aeropuerto. De acuerdo con el título de concesión, el AIFA pertenece a la SEDENA en un 99%, mientras que el 1% está en manos del Banco Nacional del Ejército.

//* ----------

170/ Rudolph, Moy, y Bedoya, Alvaro M., "Airport Face Scans".

171/ Jay Stanley, "U.S. Customs and Border Protection'sAirport Face Recognition Program", *American Civil Liberties Union* (blog), consultado el 22 de julio de 2024, https://www.aclu.org/documents/aclu-white-paper-cbps-airport-face-recognition-program

El 17 de octubre de 2019, la SEDENA inició las obras en la antigua Base Aérea Militar No. 1 "General Alfredo Lezama Álvarez". El General de Brigada Gustavo Ricardo Vallejo, encargado del proyecto, prometió al presidente "una obra de clase mundial, con la mejor tecnología y los mejores costos".[172]

El 21 de marzo de 2022, el Secretario de Defensa Nacional, Luis Crescencio Sandoval, entregó el aeropuerto en una ceremonia con el presidente Andrés Manuel López Obrador. En esta conferencia de prensa, el General Vallejo señaló que el aeropuerto "tenía que ser una infraestructura post-covid donde el pasajero privilegie el autoservicio, que el pasajero viva una experiencia *touchless* o *paperless* y que desde su propia casa o su computadora a través de reconocimiento facial haga su documentación inicial o su *check-in*".[173]

Básicamente, la SEDENA justifica que la implementación de las TRF resolvería los problemas de flujo de las personas pasajeras del AIFA, sin considerar las demás afectaciones a los derechos humanos. La SEDENA licitó y adquirió en 2021 –antes de terminar la construcción y la operación del aeropuerto– la TRF del AIFA al Consorcio Apollocom bajo el nombre "Sistema de Procesamiento de Pasajeros" (SPP) por 796 millones 929 mil 456 pesos. El contrato incluye gastos de mantenimiento solo por 24 meses, por lo que esta Secretaría tendría que incurrir en gastos adicionales para el mantenimiento del sistema una vez vencido dicho plazo.[174]

No existe un análisis previo que justifique con evidencia la necesidad de tener una herramienta tan invasiva a los derechos humanos. La SEDENA pretende sacrificar los derechos humanos de las personas usuarias por la falsa promesa comodidad de reducir filas en los aeropuertos, problema que ni siquiera se ha documentado.

Adicionalmente, el SPP recolecta de manera masiva datos personales sensibles. En un contexto donde el aeropuerto es operado y controlado indefinidamente por los militares, la figura de seguridad nacional puede ser instrumentalizada para la toma de acciones arbitrarias y aumentar los riesgos de abuso.

Una vez adquirido e instalado el sistema, el AIFA presentó una Evaluación de Impacto en la Protección de Datos Personales (EIPDP) para que el entonces Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) emitiera recomendaciones. La ley vigente establecía que estas recomendaciones no eran obligatorias para el sujeto obligado –en este caso, el aeropuerto– por lo que el AIFA decidió si las acataba o no. El AIFA decidió no seguir 46 de las 115 recomendaciones del INAI y no entregó información que garantizara que haya acatado efectivamente las recomendaciones que aceptó.

El consorcio Apollocom está conformado por las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A. de C.V., Vision-Box Soluções de Visão Por Computador S.A., y

//* ----------

172/ Revista Armas, "Primer año de Construcción del AIFA", el 2 de noviembre de 2020, consulta en: https://issuu.com/revistaarmas/docs/revistaarmas_edicionespecial_1_/s/15602473

173/ Inauguración del Aeropuerto Internacional Felipe Ángeles (AIFA). 21 de marzo de 2022. https://www.youtube.com/watch?v=3sKQOXyn5_I

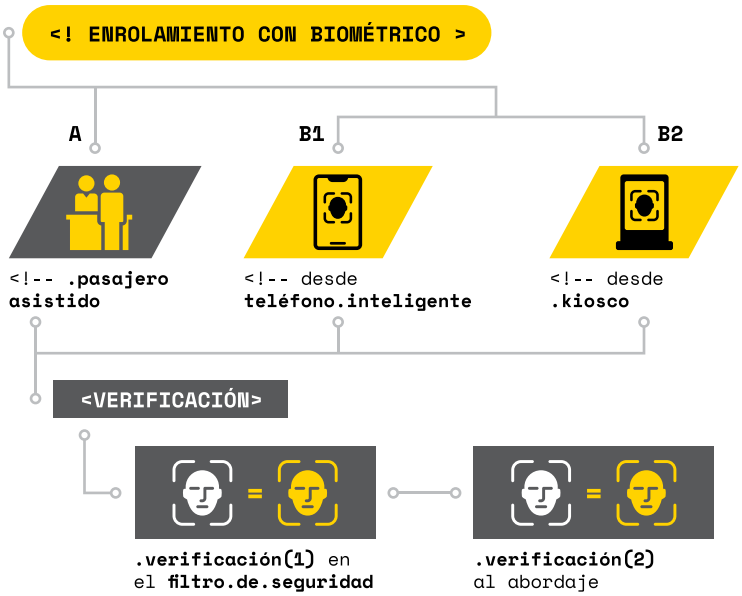
174/ Contrato Abierto entre la SEDENA y el Consorcio Apollocom pág. 6-9, obtenido por R3D de una solicitud de acceso a la información a la Secretaría de Defensa Nacional.

la empresa Amadeus IT Group. A pesar de que la información obtenida de las solicitudes de acceso a la información no fue completamente transparente sobre el rol que fungiría cada empresa en el sistema, podemos inferir según los documentos que las empresas conforman el SPP de la siguiente forma:

- Amadeus: sistema de quioscos (CUSS). Integra CUSS, CUPSS, E-gates, sistemas de las aerolíneas (pág 18, EIPDP).
- Vision box: App movil Vision-Box Mobile ID; registro manual en mostradores Vision-Box VDesk; sistema gestión de identidades VB Orchestra, un sistema de almacenamiento centralizado donde se almacenan y comparten los PDE; puertas biométricas VB Seamless Security Checkpoint eGate; puertas no biométricas eGate (de acuerdo con la propuesta técnica de Vision-Box).

FUNCIONAMIENTO DEL SISTEMA DE PROCESAMIENTO DE PASAJEROS DEL AIFA

El SPP funciona de la siguiente manera: primero, las personas usuarias tienen que registrar sus datos biométricos a través de una aplicación en su celular, en un quiosco o con una persona que le asista en los mostradores. Después las personas tienen que someterse a dos momentos de verificación, el primero durante el filtro de seguridad y el segundo durante el abordaje.



Fuente: *EIPDP del sistema de procesamiento de pasajeros del AIFA*

Para poder entrar a los filtros de seguridad, la persona debe colocarse frente a las puertas biométricas *E-Gates*. Estas puertas biométricas tomarán una foto de su cara y le identificarán para permitirle el acceso a las salas de última espera y comercios. Al momento del abordaje, la persona pasará por las puertas biométricas E-Gates situadas en esta área, las cuales tomarán nuevamente una foto de su cara y le identificarán para permitir su ingreso al avión. El sistema evalúa la elegibilidad del pasajero, lo cual implica que el acceso al avión pueda ser negado.[175]

El AIFA ha dicho que el registro biométrico es opcional. Si la persona decide no registrarse, puede pasar por los filtros de seguridad y abordaje de la manera tradicional. Sin embargo, no hay mecanismos claros para que las personas que elijan no hacer el registro biométrico puedan negarse ni hay accesos separados para quienes deciden no hacerlo. Por tanto, según informa el AIFA, las personas (con o sin registro biométrico) usarán los mismos puntos de control.

RECOLECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

¿Qué datos personales requiere el SPP?

Para hacer *check-in* en el SPP, la persona debe ingresar los datos contenidos en su pase de abordar, su identificación oficial (generalmente, el pasaporte) y una foto de su rostro. Incluso, en la opción de registro en mostradores convencionales existe la posibilidad de registrarse con la credencial de elector (INE), lo cual implicaría registrar el domicilio en el SPP. En las opciones de registro con el teléfono celular, el sistema recaba datos del dispositivo como geolocalización y actividad.

Según el Dictamen del INAI, el SPP recaba más datos de los necesarios y no cumple con el criterio de minimización de los datos y el principio de proporcionalidad.[176] En otras palabras, el SPP recolecta demasiados datos sensibles sin que exista una justificación adecuada. Por ejemplo, no se explica por qué la recolección de domicilios o datos del dispositivo de las personas pasajeras son esenciales para poder hacer ese registro.

El SPP solamente reconoce dos géneros: masculino y femenino.[177] Como mencionamos en el primer apartado, los sistemas de identificación y verificación biometrica refuerzan el binarismo de género. Este sistema excluye a personas no binaries y en general es susceptible de identificar erróneamente a personas transgénero. Un sistema que no reconoce la diversidad de identidades es susceptible de cometer más errores[178] e identificar erróneamente a alguien como una persona buscada por las autoridades.

//* ----------

175/ Evaluación de Impacto en la Protección de Datos Personales sobre el Sistema de Procesamiento de Pasajeros elaborada por el AIFA, pág 63.

176/ Dictamen sobre la Evaluación de Impacto en la Protección de Datos Personales, emitida por el INAI, 245-248.

177/ Evaluación de Impacto en la Protección de Datos Personales sobre el Sistema de Procesamiento de Pasajeros elaborada por el AIFA, pág 29.

178/ G. Macías y Luis, F. García, "La nueva cara de la discriminación: el impacto diferenciado de la tecnología de reconocimiento facial en grupos vulnerables", septiembre de 2022, 127.

Además, el AIFA no estableció los convenios necesarios para activar los servicios de verificación de la credencial del INE.[179] De acuerdo con el Dictamen del INAI, era necesario que el AIFA realizara estos convenios con el Instituto Nacional Electoral.[180] Saltarse estos convenios pone en duda la seguridad de los datos y el posible aprovechamiento de éstos para, por ejemplo, realizar prácticas de perfilamiento.

Tratamiento de datos personales

Según la información entregada por el AIFA, el SPP utiliza dos procesos para el tratamiento de datos:

a) Verificación 1:1.: Se realiza durante el registro en la app, el quiosco o el mostrador para comparar la cara de la persona con la foto de su pasaporte electrónico.

b) Identificación 1:N: Se utiliza en los filtros de seguridad y abordaje para buscar si la foto tomada en la puerta biométrica *E-Gate* coincide con algún rostro en la base de los datos de pasajeros registrados.

Según la SEDENA, el AIFA logrará el tratamiento de datos biométricos de 19.5 millones de pasajeros al año en fase 1, y 84.9 millones de pasajeros en fase 3.

En la Evaluación de Impacto que entregó al INAI, el AIFA estableció que la finalidad de obtener los datos era la de seguridad y seguridad nacional para atender requerimientos de datos de autoridades, "ya que [el sistema] permite identificar a las personas que se encuentran involucradas personas que en principio fueron pasajeros pero que realizaron o han realizado actos ilícitos graves o muy graves".[181] El INAI recomendó considerar estas finalidades, la expectativa de privacidad, la naturaleza de los datos (sensible) y las consecuencias del tratamiento.

Sin embargo, el AIFA rechazó esta recomendación y señaló que la finalidad de "dar atención al requerimiento de autoridades competentes por causas de seguridad, inclusive seguridad nacional fue errónea", y que la finalidad "correcta" era "permitir el flujo ininterrumpido sin papel, acortar tiempos de espera y evitar aglomeraciones",[182] sin dar información que asegure que las finalidades de seguridad fueron eliminadas.

//* ----------

179/ Dictamen sobre la Evaluación de Impacto en la Protección de Datos Personales, emitida por el INAI, 179 y 180.

180/ INE, "Servicio de verificación de los datos de la Credencial para Votar", *Instituto Nacional Electoral* (blog), el 6 de agosto de 2021, https://ine.mx/servicio-verificacion-datos-credencial-votar/

181/ Evaluación de Impacto en la Protección de Datos Personales sobre el Sistema de Procesamiento de Pasajeros elaborada por el AIFA, 244.

182/ Informe de implementación sobre la Evaluación de Impacto en la Protección de Datos Personales, emitida por el AIFA. Recomendación 22.

Posiblemente la rectificación de las finalidades de seguridad y seguridad nacional no sea casualidad. Estas finalidades encienden alertas sobre la seguridad de los datos y el posible aprovechamiento y explotación discrecional por parte de las autoridades. Es decir, requieren una mayor rendición de cuentas por parte del aeropuerto y es posible que esa haya sido la razón para negarla, lo cual deja duda sobre los verdaderos fines para el tratamiento de datos.

Según el INAI, todas las finalidades establecidas por el AIFA (de seguridad y de flujo de pasajeros) para implementar el SPP son contrarias a las establecidas en el Convenio sobre Aviación Civil Internacional para poder tratar datos biométricos en los aeropuertos, del cual México es parte. Este Convenio establece la posibilidad de obtener biométricos para verificar la seguridad de los documentos de viaje,[183] no para agilizar el flujo de personas en el aeropuerto ni para la seguridad nacional o prevención delictiva.

Además, el AIFA señaló que en el SPP no se podrán ejercer los derechos de acceso, rectificación, cancelación y oposición de los datos (derechos ARCO).[184] Esto significa que las personas registradas no podrán decidir sobre sus datos personales y biométricos. No podrán acceder a los datos que tiene el aeropuerto, las aerolíneas u otras entidades que reciben sus datos ni podrán corregirlos o negarse a su uso o almacenamiento. La justificación para negar estos derechos, según el AIFA, es que los datos son cifrados y disociados, y se eliminan automáticamente después del vuelo.[185]

Sin embargo, el ciclo de vida de los datos descrito por el aeropuerto no es transparente y la información a la que pudimos acceder tiene inconsistencias que dejan dudas sobre su efectiva eliminación. El AIFA dice que solo almacena los datos por un plazo máximo de 48 horas (24 horas anteriores al vuelo y 24 horas después de que salió el vuelo) pero no demuestra que cumple con los estándares para el borrado de los datos. No queda claro cuándo se realiza el bloqueo para evitar transferencias de datos ilegales ni se especifican políticas para su eliminación definitiva, lo que genera dudas sobre si los datos se borran efectivamente en el tiempo establecido.

Dado que la información está testada en varias secciones, no es posible asegurar las entidades con las que se compartirán los datos obtenidos. Mencionan que se transferirán a las aerolíneas y se compartirán con las plataformas Orchestra y Amadeus para utilizarlos en los filtros de seguridad y abordaje. No obstante, las finalidades iniciales de seguridad para la investigación de delitos y seguridad nacional implicarían, de manera inevitable, la transferencia de datos a otras autoridades.

En la información técnica entregada por la SEDENA sobre los requerimientos para contratar el sistema, podemos ver que buscaban un SPP con capacidades para el “intercambio

//* ----------

183/ Anexo 9 del Convenio sobre Aviación Civil Internacional, capítulo 3c https://www.gob.mx/cms/uploads/attachment/file/603834/anexo-9.pdf

184/ Respuesta a solicitud de acceso a la información 1100-2024 numeral 37 realizada por R3D al Aeropuerto Internacional Felipe Ángeles.

185/ Justificación por la que no se aceptan las recomendaciones número 26, 27, 28, 30, 36, 49, 95, 96, 97, 98 en el Informe de implementación.

de datos de pasajeros",[186] por lo que es posible que otras transferencias no mencionadas estén planeadas.

ETAPA DE ENROLAMIENTO

Registro vía aplicación móvil

La persona usuaria debe instalar la aplicación móvil del AIFA para hacer el registro. El aviso de privacidad[187] no especifica los datos que se obtendrán del dispositivo móvil al descargar la aplicación. Sin embargo, además de los datos personales para registrarse en el SPP, podrían obtenerse datos de geolocalización y de la actividad del dispositivo.

La verificación 1:1 compara la fotografía obtenida con la del chip del pasaporte electrónico y la fotografía capturada por la persona desde su dispositivo móvil. De confirmarse que la selfie y la fotografía del pasaporte coinciden, se genera el registro (un *Passenger Data Envelope*). Como mencionamos anteriormente, los datos obtenidos de la *app* se transferirán a las aerolíneas y se compartirán con las plataformas Orchestra y Amadeus para que puedan utilizarse en los filtros de seguridad y abordaje, sin que exista certeza sobre si los datos son compartidos y almacenados por otras entidades.

Registro vía quioscos

El Sistema de Autoservicio de Uso Común (CUSS) de Amadeus consiste en quioscos donde los pasajeros pueden hacer su registro biométrico sin asistencia. Al igual que en las apps, los quioscos hacen una comparación 1:1 entre la foto del pasaporte electrónico y la foto del pasajero capturada en el quiosco. Los datos obtenidos se transferirán a las aerolíneas y se compartirán con las plataformas Orchestra y Amadeus para que puedan utilizarse en los filtros de seguridad y abordaje, sin que exista certeza sobre si los datos son compartidos y almacenados por otras entidades.

Registro vía mostradores

El Sistema de Uso Común para el Procesamiento de Pasajeros (CUPPS) son los mostradores convencionales donde el pasajero puede hacer su registro biométrico con ayuda del personal de la aerolínea. El personal toma la foto de la persona con la cámara del mostrador, la cual hace una comparación 1:1 para verificar la identidad de la persona con la foto del chip del pasaporte. Como mencionamos, en esta opción también mencionaron que es posible el registro con la credencial del INE, lo cual llamó la atención del INAI ante la falta de convenios previos con este instituto.

//* ----------

186/ Ficha técnica de la SEDENA respecto a la contratación del Sistema de Procesamiento de Pasajeros, 71 y 72.

187/ Aviso de privacidad integral de la app del Sistema de Procesamiento de Pasajeros. https://aifa-repositorio.s3.amazonaws.com/UnidadTransparencia/Avisos+de+privacidad+integrales/AVISO+DE+PRIVACIDAD+INTEGRAL+APP.pdf

ETAPA DE VERIFICACIÓN

Primer paso. La verificación en filtros de seguridad

Para entrar a los filtros de seguridad, la persona usuaria se colocará frente la puerta biométrica *E-Gate*, la cual tomará una foto para validarla con aquella que fue tomada al momento del registro en la aplicación, el quiosco o el mostrador. Una vez que la puerta biométrica valida el acceso la persona ingresará a los filtros de seguridad. Pasado este filtro, podrá acceder al área de comercios y a las salas de última espera.

Segundo Paso. Verificación al abordar

Al momento del abordaje, la persona pasará por las E-Gates que lo identificarán nuevamente para permitir su ingreso al avión. El AIFA menciona que las E-Gates evalúan "la elegibilidad del pasajero", por lo que el ingreso a los filtros de seguridad o al abordaje puede ser negado.

La información que entregó el AIFA no incluye los pasos a seguir en caso de que la tecnología cometa errores, como la identificación incorrecta de personas. Tampoco habla de los procedimientos a seguir en caso de que el sistema arroje falsos positivos o falsos negativos ni de la rendición de cuentas que surgiría en caso de que una persona no pueda ingresar a un vuelo debido a estos resultados. Esto refuerza la incertidumbre en torno a la seguridad de las personas y sus datos en la operación del SPP.

¿QUÉ TAN CONFIABLE ES EL SPP?

La confianza en el uso de TRF y sistemas de identificación biométrica se refiere a distintos factores:

01// ¿Qué tan preciso técnicamente es este sistema?

02// ¿El AIFA analizó adecuadamente los riesgos de estos sistemas en los derechos de las personas?

Precisión del sistema de verificación usado por el AIFA

Como expusimos en el primer capítulo, la TRF no es exacta. Las precisión de los sistemas con capacidad de reconocimiento facial varían dependiendo de cada algoritmo. En Estados Unidos, el Instituto Nacional de Estándares y Tecnología (en adelante, NIST, por sus siglas en inglés) se encarga de analizar los múltiples sistemas de TRF creados por diversas empresas. En su Evaluación de tecnología de reconocimiento facial (1:1 verificación) analizaron 192 algoritmos y sus distintas tasas de error.[188]

//* ----------

188/ Instituto Nacional de Estándares y Tecnología. Face Recognition Technology Evaluation (FRTE) 1:1 Verification. 09 de agosto de 2024. Consulta en: https://face.nist.gov/frte/reportcards/11/visionbox_005.html

En este caso, el AIFA utiliza el sistema de verificación desarrollado por la empresa Vision Box. Dentro del análisis de NIST de los sistemas de Vision Box se encontraron los siguientes datos relevantes:

- Los algoritmos de Vision Box relacionados con los quioscos más recientes están clasificados en los puestos 169 y 122, de aproximadamente 570 algoritmos.
- El sistema de Vision Box se equivoca 5:1 verificando la identidad de hombres racializados en comparación con hombres caucásicos. De igual forma, se equivoca 6:1 verificando la identidad de mujeres racializdas en comparación con mujeres blancas.

Dentro de las solicitudes de acceso a la información que realizamos, le preguntamos a las autoridades a cargo del AIFA sobre la tasa de error. El AIFA respondió que la tasa de error es de 0.4 por 100,000 transacciones en referencia a la *false accept rate* en un entorno controlado. Sin embargo, las respuestas son engañosas.

El *false accept rate* se refiere a cuántas veces el sistema aceptó a la persona impostora. En otras palabras, cuántas veces el sistema identifcó a una persona usando credenciales fraudulentas. No nos dicen cuántas veces el sistema identifica como impostora a las personas que sí son quienes dicen ser. Tomando en cuenta que el sistema tiene un sesgo hacia las personas racializadas, existe la posibilidad que este sistema identifique a una persona racializadas como impostora por un error en la verificación de credenciales.

Proceso de Evaluación de Impacto en la Protección de Datos

R3D también solicitó vía transparencia el documento de la evaluación de impacto a la privacidad. Si bien en principio el AIFA negó la entrega de este documento, el INAI resolvió un recurso de revisión a nuestro favor para poder acceder a esta información.

La Evaluación entregada por el AIFA contenía información crucial reservada. Datos relacionados con los nombres de las plataformas y tecnologías que serán utilizadas se encuentran clasificadas como reservadas debido a que “si se diera a conocer, podría poner en riesgo la prevención” de delitos.[189] Incluso, dentro del escueto análisis de proporcionalidad, se encuentran testadas las características generales que dotarían de mayor privacidad “por diseño”.

Adicionalmente, dentro de la evaluación de impacto a la privacidad se realiza un deficiente estudio de idoneidad y necesidad. Los argumentos solo se dedican a reiterar que esta tecnología se usará para mejorar el flujo de pasajeros y la seguridad del aeropuerto. En ninguna parte del documento se refieren a las salvaguardas que tendrá el sistema de procesamiento de pasajeros para efectivamente proteger datos tan sensibles como los datos biométricos. Incluso, el AIFA no analiza propiamente la proporcionalidad, simplemente se refiere a que

189/ Evaluación de Impacto en la Protección de Datos Personales, Sistema de Procesamiento de Pasajeros del Aeropuerto Internacional “Felipe Ángeles”. Página 51-53.

estas medidas son equilibradas. El AIFA menciona que existe un balance entre facilidad y seguridad pero nunca explica cómo realmente se logra ese equilibrio.

El aeropuerto también reservó porciones significativas de la información por formar parte de "un proceso deliberativo que no había concluido". Sin embargo, esta razón de reserva resultaba engañosa porque la ley vigente no determinaba el momento de conclusión de las Evaluaciones de Impacto a la Privacidad. Las recomendaciones emitidas por el INAI no eran obligatorias y, por tanto, no era posible determinar su conclusión con certeza.

Gracias a un juicio de amparo promovido por R3D, donde cuestionamos los criterios sobre el inicio y conclusión de este tipo de evaluaciones por no estar expresado en las disposiciones vigentes, la Jueza Décimoséptima en Materia Administrativa en la Ciudad de México ordenó al INAI que no convalidara las razones de reserva del AIFA.[190]

La jueza determinó que:

> La información de que se trata tiene que ver con el tratamiento de datos personales, el cual, desde la perspectiva de esta juzgadora, permite justificar la necesidad de hacer prevalecer la difusión y la transparencia, máxime que no se advierte que resulten afectados los intereses nacionales, los de la sociedad o derechos de terceros, pues el conocer la información respecto al tratamiento de datos personales (en específico, sus datos biométricos) implica de hecho, una necesidad fáctica de la sociedad, lo que va más allá de la implementación de determinadas recomendaciones. (...) , el no conocer respecto del tratamiento que se le dará a los datos biométricos y dada su sensibilidad e importancia, como lo precisa la parte quejosa, implica el riesgo de que la ciudadanía no conozca el alcance de la tecnología a utilizarse, ello con independencia que al momento, se hayan o no adoptado las recomendaciones que el INAI efectuó al AIFA.

De esta forma, desestimó el argumento de mantener la reserva por tratarse de un proceso aún en trámite. A pesar de que la concesión de este amparo fue impugnada por el INAI, la magistrada del Decimosexto Tribunal Colegiado en Materia Administrativa del Primer Circuito confirmó la decisión de la jueza de otorgar este amparo a favor de R3D.[191] En consecuencia, el aeropuerto se encuentra legalmente obligado a entregar dicha información que, al cierre de la edición de este documento, nos encontramos en espera de recibir y analizar.

Cabe mencionar que la deliberación de la evaluación de impacto a la privacidad se realizó sin ninguna apertura a sociedad civil o academia. A pesar de estar tratando con herramientas sumamente invasivas, se dejó fuera de la conversación a partes interesadas que pudieran pro-

//* ----------

190/ Disponible en: https://archivo.r3d.mx/wp-content/uploads/2025/06/AIFA-juzgado.pdf

191/ Disponible en: https://archivo.r3d.mx/wp-content/uploads/2025/06/AIFA-TCC.pdf

veer su experiencia o consejo para salvaguardar de mejor manera la privacidad de las personas usuarias. Por ello, aunque exista un mandato legalmente vinculante para que el AIFA dé a conocer la información, las preocupaciones en materia de derechos humanos prevalecen.

EL SISTEMA DE PROCESAMIENTO DE PASAJEROS PONE EN RIESGO LOS DERECHOS HUMANOS

Privacidad y protección de datos personales

La TRF en aeropuertos viola la privacidad y la protección de datos de las personas usuarias. Estos sistemas exigen la recopilación y procesamiento masivo de una amplia lista de datos personales por parte de proveedores de tecnología, aerolíneas y entidades públicas que operan los aeropuertos. La persona usuaria pierde el control de sus datos bajo la promesa de que pasará por filas más cortas en los filtros.

En el contexto de aeropuertos, no existe certeza sobre la verdadera intención para el tratamiento de datos. Las finalidades de seguridad o seguridad nacional en las que se han basado aeropuertos como el AIFA no son fines válidos bajo los convenios internacionales. Los fines de seguridad implican inevitablemente la transferencia de datos a autoridades para cumplir con sus requerimientos, lo que plantea dudas sobre si los aeropuertos realizarían transferencias de datos a autoridades u otras entidades, y lo que estas podrían hacer con ellos.

Un ejemplo de estos potenciales abusos ocurrió el 22 de enero de 2025, cuando el presidente de la Mesa Directiva del Senado, Gerardo Fernández Noroña, publicó un vídeo tomado por las cámaras del Aeropuerto Internacional de la Ciudad de México (AICM) para exhibir a un hombre que le habría robado un paquete.[192] El legislador fue cuestionado sobre cómo obtuvo la grabación, a lo que hizo caso omiso. La entonces comisionada del INAI, Julieta del Río, declaró a la prensa que el AICM faltó a su deber de confidencialidad y que "sí hubo abuso entre autoridades".[193]

Otras finalidades que suelen ser invocadas por los aeropuertos, como la agilización del flujo de personas pasajeras, no son suficientes para justificar la implementación de una TRF. Ese es el caso del AIFA, donde antes de comenzar las operaciones del aeropuerto y verificar que las aglomeraciones podrían ser un problema, la SEDENA adquirió, instaló y puso a prueba el sistema sin haber convalidado que la seguridad de las personas y sus datos estaría garantizada con una TRF, pues la EIPDP fue presentada después de realizar todas estas gestiones.

En el caso del AIFA, para registrarse es necesario el pasaporte, el pase de abordar y, en

//* ----------

192/ Cortés, JC. 22 de enero de 2025. "Fernández Noroña acusa a un hombre de robarle carne; cuestionan cómo obtuvo video del AICM". *Proceso*. https://www.proceso.com.mx/nacional/2025/1/22/fernandez-norona-acusa-un-hombre-de-robarle-carne-cuestionan-como-obtuvo-video-del-aicm-344223.html

193/ Ballardo, I. 23 de enero de 2025. "'Hubo abuso entre autoridades': INAI confirma complicidad entre Fernández Noroña y el AICM". *Publimetro*. https://www.publimetro.com.mx/noticias/2025/01/23/hubo-abuso-entre-autoridades-inai-confirma-complicidad-entre-fernandez-norona-y-el-aicm/

algunos casos, el uso de un dispositivo móvil. Esto implica la recolección de datos que van más allá de los biométricos, como el género, la fotografía del pasaporte, la geolocalización y la actividad del dispositivo. La creación de una base de datos con esta información, sin garantías sobre la seguridad ni transparencia en su manejo y borrado efectivo, pone en grave riesgo las libertades individuales.

La vulneración y explotación de estos datos puede resultar en consecuencias irreversibles, como la suplantación de identidad, y facilita prácticas de perfilamiento que violan derechos humanos. Además, el almacenamiento de datos biométricos y personales por parte de autoridades fomenta un ecosistema de vigilancia masiva que puede ser reutilizado y replicado en otros contextos.

Tanto en México como en muchos otros países, el responsable que trate datos personales debe garantizar que las personas puedan disponer de sus datos personales (derechos ARCO). Esto implica que puedan acceder a sus datos que están en manos de cierta entidad, que puedan revocar (anular) su consentimiento, cancelar sus datos (solicitar su eliminación) u oponerse a que se traten para ciertos fines. Sin embargo, el AIFA decidió unilateralmente que los derechos ARCO no pueden ser ejercidos en el SPP. El no tener que rendir cuentas sobre la protección de los datos posibilita otras arbitrariedades.

En este contexto, la persona pierde toda expectativa de privacidad porque no puede ejercer ningún control sobre sus datos una vez que los registra. La pérdida de control sobre los propios datos y los riesgos asociados a la entrega de estos violenta la privacidad y la protección de datos personales.

LIBERTAD DE EXPRESIÓN Y REUNIÓN PACÍFICA

La TRF en aeropuertos inhibe la libertad de expresión. Los datos sensibles obtenidos de cada persona llevan a la creación de perfiles, patrones y supuestas predicciones respecto a todas las personas registradas. De esta forma, las TRF pueden ser utilizadas para reprimir a quienes usan los aeropuertos.

Un ejemplo de esto sería el sesgo predeterminado de que “las personas con ciertos rasgos faciales y vestidas de cierta manera pertenecen a cierta etnia, y las personas que pertenecen a esta etnia son más propensas a involucrarse en el tráfico de drogas”. Esto generaliza y estigmatiza a ciertos grupos y genera consecuencias para toda persona que cumpla con estas características. Estas consecuencias pueden incluir la detención ilegal de estas personas o la revisión adicional en los filtros de seguridad.

En México existe información que apunta que la TRF y la videovigilancia es utilizada para reprimir a personas opositoras del gobierno. En diciembre de 2023, la politóloga Denise Dresser publicó en su cuenta de X sobre su inconformidad ante la saturación en el área de migración del AICM, pese a estar en manos de las fuerzas armadas.[194]

//* ----------

194/ Denise Dresser (@DeniseDresserG). X, 19 de agosto 2023. https://x.com/DeniseDresserG/status/1736983309635166643

La cuenta oficial de X del AICM le respondió públicamente con información detallada sobre su proceso por el aeropuerto; desde la colocación de su avión en el túnel de posición hasta el tiempo que pasó en migración y la hora en que salió del aeropuerto. Denise Dresser condenó esta publicación y señaló que se trataba de "un abuso de poder y una violación de la Ley General de Datos Personales en Posesión de Sujetos Obligados".[195]

Cualquier persona en situación de movilidad, incluyendo a periodistas y opositoras del gobierno, es susceptible de sufrir represiones a través de la TRF por la manera en que se expresa. El miedo a ser víctima de actos arbitrarios por parte de las autoridades en los aeropuertos debido al tratamiento de datos puede cambiar la manera en la que una persona expresa su religión, ideología política, identidad, orientación sexual, opiniones personales, preferencias culturales, entre otras cuestiones.

Igualdad y no discriminación

Los sesgos trasladados a las TRF, las prácticas de perfilamiento y las tasas de error de los sistemas impactan negativamente a grupos en situación de vulnerabilidad, como personas de color, personas indígenas, mujeres o personas de la comunidad LGBTTTIQ+.

El impedimento a ejercer derechos humanos por cumplir con ciertas características físicas, origen étnico, género, nacionalidad, religión, preferencias, entre otras, es discriminatorio y, como hemos reiterado, puede hacer a las personas bajo estas categorías sean víctimas de distintos actos arbitrarios.

Un ejemplo de esto podría ser el sesgo predeterminado de que "las personas de cierta nacionalidad son más propensas a migrar sin documentación oficial, por lo que es posible que presenten documentos falsos", lo cual generaría retenciones adicionales de personas que, según la TRF, se adecuen a ese "perfil". De este modo, las prácticas discriminatorias en los aeropuertos que han afectado tradicionalmente a ciertos grupos se amplifican y perpetúan mediante las TRF, lo cual convierte a esta tecnología en un instrumento de exclusión a gran escala.

En Estados Unidos, la TRF de la compañía Clearview –que obtiene imágenes de rostros de redes sociales y fuentes públicas– ha sido utilizada por autoridades como el Servicio de Inmigración y Control de Aduanas (ICE) y el Departamento de Justicia; el Departamento de Seguridad Nacional (DHS), el Buró Federal de Investigación (FBI), la Oficina de Aduanas y Protección Fronteriza (CBP) y la Interpol para buscar a personas de interés. Por ejemplo, ICE usó esta TRF para hacer búsquedas en bases de datos de licencias de manejo e identificar migrantes para deportarlos.[196] Esta tecnología también es usada en Emiratos Árabes Unidos o Arabia Saudita, países donde se criminaliza la homosexualidad; y específicamente en

//* ----------

195/ Denise Dresser (@DeniseDresserG). X, 19 de agosto 2023. https://x.com/DeniseDresserG/status/1737215595123253614

196/ Jarrahi, Javad. "ACLU Suit Seeks the Release of Clearview AI Face Biometrics Data by ICE and CBP." Biometric Update, April 16, 2021. https://www.biometricupdate.com/202104/aclu-suit-seeks-the-release-of-clearview-ai-face-biometrics-data-by-ice-and-cbp

este último, ha sido usado por parte de la policía.[197]

Los grupos que se han visto tradicionalmente discriminados en los aeropuertos, como personas racializadas, migrantes, personas trans y aquellas con preferencias religiosas o culturales específicas sufren mayores riesgos de discriminación con el uso de reconocimiento facial. Los aeropuertos suelen implementar las TRF bajo los pretextos de seguridad y seguridad nacional, lo que implica la transferencia de datos a autoridades de seguridad. Esto amplifica el riesgo de discriminación, ya que refuerza los sesgos existentes y permite un perfilamiento aún más invasivo de estos grupos que se reproduce más allá de los aeropuertos.

Presunción de inocencia

La TRF en aeropuertos viola la presunción de inocencia porque trata a todas las personas como sospechosas. En los aeropuertos, una TRF propicia actos arbitrarios como interrogatorios injustificados a personas que se adecuan a cierto perfil, acoso u otras situaciones adversas a las que los grupos estigmatizados tendrían que enfrentar injustamente. Estas arbitrariedades muestran la facilidad con la que los operadores de estos sistemas pueden asumir como culpable a cualquier persona de cualquier cosa, incluso de actividades que no se traten de un delito, sino de expresiones o actos que resultan incómodos para las autoridades.

La implementación de TRF facilita la creación de listas de vigilancia o listas negras que pueden interoperar con las bases de datos de otras agencias de gobierno. Esto aumenta el riesgo de estigmatización de grupos marginados y vulnerables y abre la puerta a una vigilancia permanente por parte del Estado que considera culpables a todas las personas hasta que se demuestre lo contrario.

//* ----------

197/ Mac, Ryan, Albert Fox Cahn, and Alyssa D. Morrow. "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA". BuzzFeed News, February 26, 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement

CAP.04\\

RECONOCIMIENTO FACIAL EN ESTADIOS: NUESTROS DERECHOS EN JUEGO

El fútbol en México celebra 457 partidos por torneo en sus tres ligas (Liga MX varonil, Liga MX femenil y Liga de Expansión). A la mitad del torneo Clausura 2024, 2.83 millones de personas habían asistido a los estadios, la cifra más alta reportada desde el torneo Apertura 2019, previo a la pandemia por COVID-19.[198]

La creciente de asistencia a estos recintos, la rivalidad entre equipos y las vinculaciones emocionales en este deporte lo convierte en una de las principales fuentes culturales y recreativas en nuestro país, pero también en un entorno que puede motivar comportamientos extremos. La violencia en el fútbol mexicano ha desencadenado actos de discriminación, incluyendo gritos homofóbicos, y eventos altamente violentos, como riñas e incluso muertes en los estadios.

El 5 de marzo de 2022, el Estadio Corregidora de Querétaro fue sede de un acontecimiento de violencia sin precedentes en el partido entre los *Gallos Blancos* de Querétaro contra los *Zorros* del Atlas. Según cifras oficiales, las agresiones brutales dejaron al menos 26 personas heridas, tres de ellas gravemente, sin reportar ningún fallecimiento. Estas cifras fueron objeto de polémica y cuestionamientos, pues testimonios de personas que estuvieron en el Corregidora aseguraron que sí hubo muertes y señalaron la ausencia de elementos de seguridad que impidieran la violencia.

Las TRF y los sistemas de identidad digital han sido utilizados en eventos masivos alrededor del mundo, tales como ligas deportivas nacionales, la Copa Mundial de Fútbol, Juegos Olímpicos e incluso conciertos. Estos proyectos han buscado justificarse en objetivos como agilizar las entradas a los estadios, instaurar métodos de pago contactless y mejorar la seguridad. De los 100 estadios más importantes del mundo, 25 usan TRF, y cada vez más recintos incorporan estas tecnologías.[199]

Las instituciones deportivas, gobiernos y empresas que han propuesto la implementación de estos proyectos aseguran que con el registro obligatorio de todos los asistentes podrán dar con quienes emiten el grito homofóbico o cometen actos violentos, lo cual garantizaría mayor seguridad. Sin embargo, la obligación de hacer un registro biométrico para ingresar

//* ----------

198/ Estadio Deportes. ¡Estadios llenos! Liga MX registra su mejor asistencia desde la pandemia. 11 de abril de 2024.https://www.estadiodeportes.mx/ligamx/Estadios-llenos-Liga-MX-registra-su-mejor-asistencia-desde-la-pandemia-20240411-0053.html

199/ Moody, R. Surveillance Camera Statistics: Which Football Fans Are the Most Watched in the World? Comparitech. 6 de septiembre de 2023. https://www.comparitech.com/blog/vpn-privacy/the-worlds-most-surveilled-football-stadiums/

a un estadio conlleva el sometimiento a los daños que generan las TRF en nuestros derechos humanos.

Estas afectaciones se materializan cuando le impiden a una persona entrar al estadio porque la identificaron erróneamente como un criminal; al ser objeto de sanciones o detenciones por resultados equivocados del sistema con sesgos discriminatorios; o cuando los datos de las personas sean compartidos de forma indiscriminada con instituciones, gobiernos y empresas, sin que se conozca qué harán con ellos. De esta forma, las personas deben convertirse en sospechosas hasta demostrar lo contrario para poder ingresar a los recintos deportivos.

Bajo la falsa premisa de que la tecnología soluciona todo –incluso los problemas de violencia–, la TRF ha sido implementada en México desde 2022 en partidos de fútbol. Pese a esta implementación, la violencia no ha disminuido; los actos violentos en el fútbol mexicano aún suceden de manera recurrente. Por lo tanto, los derechos humanos de las personas que asisten a estos eventos han sido sacrificados a cambio de un proyecto que no ha solucionado los problemas para los que fue implementado.

En este capítulo analizaremos la implementación de estos sistemas en estadios alrededor del mundo, así como las opiniones de distintas jurisdicciones al respecto. Después, evaluaremos el caso del "Fan ID" en México y su verdadera efectividad como una solución para los problemas de violencia. Finalmente, señalaremos los enfoques que pueden ser útiles para encontrar soluciones menos riesgosas e invasivas para los derechos de quienes asisten a estos eventos.

En la implementación de reconocimiento facial, no cabe confundir necesidad con conveniencia de la organización - Agencia Española de Protección de Datos, sobre la adquisición de TRF por parte de LaLiga.

RECONOCIMIENTO FACIAL EN ESTADIOS: UNA MIRADA GLOBAL

La TRF se ha implementado alrededor del mundo bajo la falsa premisa de seguridad o eficiencia. Según el gobierno de Japón, en los Juegos Olímpicos y Paralímpicos de Tokio 2020, la TRF fue utilizada para identificar a 300 mil personas. Este sistema, provisto por la empresa NEC, incluía un sistema de identidad digital que generaba tarjetas de identificación para permitir el ingreso y cámaras de vigilancia con TRF. Estas cámaras registraban la temperatura facial para detectar síntomas de coronavirus, así como la superficie corporal para comprobar si las personas llevaban mascarillas.[200]

Durante el mundial de Rusia 2018, los resultados arrojados por más de 450 cámaras de reconocimiento facial de la empresa rusa NtechLab provocaron la detención de más de 180

//* ----------

200/ Tokyo 2020: All is Ready for a Safe and Secure Tokyo 2020 Games. Government of Japan, 2019. https://www.japan.go.jp/tomodachi/2019/autumn-winter2019/tokyo2020.html

personas, a las cuales se les prohibió la entrada a los partidos del evento. Entre estos "infractores" se encontraban activistas de oposición.[201] Después del mundial, la vigilancia con TRF se siguió utilizando en eventos deportivos y en el metro para detener y amedrentar a personas buscadas por el gobierno, como activistas, periodistas y opositores, razón por la cual Rusia fue sancionada en 2023 por el Tribunal Europeo de Derechos Humanos.[202]

El sistema utilizado en Rusia 2018 también fue implementado en Catar 2022, donde se desplegaron más de 22 mil cámaras con reconocimiento facial y más de 200 mil "unidades integradas" –como drones– para vigilar los ocho estadios mundialistas y las calles de Doha. En un centro de mando, más de 100 técnicos vigilaban a las personas y podían hacer acercamientos al rostro de cada uno de los 60 mil espectadores que asistían en promedio. Enfocar el rostro de cada persona les permitía "captar su información" y "predecir los patrones de las multitudes",[203] lo cual ayudó a identificar e intimidar a personas que utilizaban la bandera de la comunidad LGBTTTIQ+.[204]

Además, en ese Mundial los asistentes debían descargar dos aplicaciones: Ehteraz, un rastreador de COVID-19; y Hayya, que pedía el registro de datos biométricos para poder acceder a los estadios y al transporte público. Ehteraz tenía acceso a las fotos y vídeos de los usuarios y solicitaba la activación de servicios de localización en segundo plano. Tom Lysemose Hansen, cofundador de Promon –una empresa de seguridad de aplicaciones– señaló que "es claro que la app [tomaba] datos del usuario final por más razones que las expresadas por el botón de consentimiento",[205] lo cual generó dudas sobre el uso de los datos obtenidos en estas apps.

Desde 2024, varios estadios de la Major League Baseball (MLB) han implementado reconocimiento facial para agilizar el ingreso a través del programa "Go-Ahead Entry". Organizaciones de derechos humanos, como *Fight for the Future* y *Access Now*, protestaron contra la puesta en marcha de este sistema debido a los sesgos y errores de este tipo de tecnologías.

Las organizaciones afirmaron que "a medida que esta tecnología se extienda a más estadios, solo veremos más casos de identificación errónea traumática que afectarán a personas de color, mujeres y personas no conformes con su género".[206] También cuestionaron el

//* ----------

201/ Light, F. "Russia Is Building One of the World's Largest Facial Recognition Networks." *Coda Story*, 8 de noviembre de 2019. https://www.codastory.com/authoritarian-tech/russia-facial-recognition-networks/

202/ European Court of Human Rights. *H.F. and Others v. France*. No. 001-225655. HUDOC, 14 de septiembre de 2022. https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}

203/ Lusweti, S. "Towards the Advanced Technology of Smart, Secure, and Mobile Stadiums: A Perspective of FIFA World Cup Qatar 2022." ResearchGate. enero 2023. https://www.researchgate.net/profile/Samuel-Lusweti/publication/375525907_Towards_the_Advanced_Technology_of_Smart_Secure_and_Mobile_Stadiums_A_Perspective_of_Fifa_World_Cup_Qatar_2022/links/654df5c1b86a1d521bc8b037/Towards-the-Advanced-Technology-of-Smart-Secure-and-Mobile-Stadiums-A-Perspective-of-Fifa-World-Cup-Qatar-2022.pdf

204/ Wahl, G. "An Unexpected Detention by World Cup Security." Substack, 13 de diciembre de 2022. https://grantwahl.substack.com/p/an-unexpected-detention-by-world

205/ World Cup Security: World Cup apps pose a data security and privacy nightmare. The Register, 11 de noviembre de 2022. https://www.theregister.com/2022/11/11/world_cup_security/

206/ Fight for the Future, Letter to Major League Baseball, team owners, venue owners, sports leagues, and all leaders in professional sports. s/f https://www.fightforthefuture.org/news/2023-09-26-bfr-stadiums/

verdadero peso del consentimiento de las personas que entregan sus datos, ya que eligen no hacerlo y deben enfrentarse a filas muy largas como consecuencia.

Recintos como el Madison Square Garden y el Radio City Music Hall en Nueva York han implementado TRF para identificar a personas abogadas que trabajan o han trabajado en despachos jurídicos involucrados en litigios contra las empresas del propietario, James L. Dolan.[207] En las "listas de exclusión" de estos recintos se encuentran cientos de estas personas, cuyas caras fueron obtenidas de los sitios web de los bufetes de abogados donde trabajan. Un algoritmo examina instantáneamente estas imágenes y sugiere coincidencias, lo cual permite su identificación y restricción de acceso a estos eventos.

En 2020, el Tribunal de Apelaciones de Cardiff determinó como ilegal el sistema de reconocimiento facial utilizado por la policía de Gales del Sur en partidos de fútbol y conciertos. [208] Esto se debe a que la policía no evaluó adecuadamente los riesgos que la tecnología representaba para los derechos humanos. La policía desconocía el conjunto de datos con el que se había "entrenado" la tecnología, por lo que no podía determinar si había existido un desequilibrio demográfico en los datos usados para entrenar el algoritmo.

Por otro lado, en 2021 la Agencia de Protección de Datos de Francia emitió una advertencia al club Metz para detener el uso de TRF y determinó esta práctica como ilegal,[209] pues bajo ciertas excepciones en el Reglamento General de Protección de Datos de Europa (RGPD) es una práctica prohibida. Para asegurar el acato de esta advertencia, esta agencia estableció la posibilidad de imponer una multa en caso de incumplimiento.

En Argentina, el programa Tribuna Segura 2.0 –que incluye TRF en los estadios– inició en 2018 para "poner a disposición de la justicia" a las personas que fueran identificadas en caso de dar positivo. A raíz de este programa, el ministerio de seguridad creó el Registro Nacional de Personas con Derechos de Admisión en Espectáculos Futbolísticos, el cual fue compartido con Estados Unidos en la Copa América de 2024 para la "prevención de incidentes violentos".[210]

En la final de la Copa América 2024 en el partido de Colombia contra Argentina, ocurrieron disturbios violentos tras las aglomeraciones generadas en la entrada al Hard Rock Stadium de Miami. Las autoridades locales utilizaron TRF para buscar a los más de siete mil hinchas que presenciaron el suceso, bajo la amenaza de tomar medidas de prisión o deportación.

//* ----------

207/ Hill, K. y C. Kilgannon. Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies. *The New York Times*. 22 de diciembre de 2022. https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html

208/ R (Bridges) v. Chief Constable of South Wales Police and Others. [2020] EWHC 2536 (Admin). High Court of Justice, 2020. https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

209/ Roseman, M. French watchdog warns sports club about unlawful use of facial recognition technology. Reuters. 18 de febrero de 2021. https://www.reuters.com/article/sports/french-watchdog-warns-sports-club-about-unlawful-use-of-facial-recognition-techn-idUSKBN2AI2M9/

210/ Resolución 447/2024 - Secretaría de Asuntos Estratégicos." Boletín Oficial de la República Argentina, 8 de mayo de 2024. https://www.boletinoficial.gob.ar/pdf/aviso/primera/306938/20240508

[211] Esta situación plantea preocupaciones sobre el uso de datos sensibles obtenidos en contextos locales específicos para fines migratorios y su transferencia entre países, como Argentina, Colombia y Estados Unidos, en este caso.[212]

Este tipo de acciones aumentan las preocupaciones al considerar que la TRF instalada en la ciudad de Buenos Aires fue declarada inconstitucional en 2022 gracias a los esfuerzos de organizaciones de la sociedad civil como el Observatorio de Derecho Informático Argentino (ODIA) y la Asociación por los Derechos Civiles (ADC). El sistema fue impugnado porque no cumplía con estándares adecuados y por el uso indebido de los datos personales, ya que incluso personas que no eran buscadas por la justicia fueron detenidas.[213]

En Brasil, el Ministerio de Justicia y Seguridad Pública y la Confederación Brasileña de Fútbol implementaron el proyecto "Estadio Seguro" con TRF para perseguir delitos y compartir los datos de quienes asisten a los estadios con la policía. Al respecto, la Autoridad Nacional de Protección de Datos brasileña (ANPD) emitió una nota técnica.[214]

Uno de los principales cuestionamientos en esta nota técnica fue el periodo de 50 años para almacenar los datos personales "para fines de inteligencia". Para la ANPD, "no tiene sentido someter los datos recogidos de ciudadanos que están ejerciendo plenamente sus derechos y no son objeto de actividades de seguridad pública a un tratamiento que llevaría a su conservación durante 50 años o más". Para esta agencia, un proyecto así implica el riesgo de establecer una vigilancia exacerbada por parte del Estado.

Otra preocupación de la ANPD fue la poca claridad de la información proporcionada sobre el tratamiento de datos biométricos y las comparticiones de datos con otros entes públicos y privados. También alertaron sobre las deficiencias en las medidas de mitigación y tratamiento de riesgo. Dadas estas cuestiones, la ANPD pidió que se acreditara el cumplimiento de los ajustes necesarios para que el proyecto fuera acorde a la ley.

En España, la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia propuso que los clubes instalaran sistemas biométricos para controlar el acceso a los estadios. Pese a que desde 2022 estos sistemas ya se estaban implementando en estadios como el Sadar de Osasuna, a inicios de 2023, la Agencia Española de Protec-

//* ----------

211/ Donald Trump ordenaría deportaciones masivas de colombianos involucrados en los disturbios en la final de la Copa América 2024. 1 de febrero 2025. https://www.infobae.com/colombia/2025/02/01/donald-trump-ordenaria-deportaciones-masivas-de-colombianos-involucrados-en-los-disturbios-en-la-final-de-la-copa-america-2024/

212/ U.S. and Colombia Agree to Share Biometric Data of Immigrants, 28 de marzo 2025. https://www.democracynow.org/2025/3/28/headlines/us_and_colombia_agree_to_share_biometric_data_of_immigrants

213/ O.D.I.A. y Otros contra Gobierno de la Ciudad Autónoma de Buenos Aires. Amparo - Otros. Repositorio del Ministerio Público de la Defensa, 7 de septiembre de 2022. https://repositorio.mpd.gov.ar/jspui/bitstream/123456789/4658/1/O.D.I.A.%20Y%20OTROS%20CONTRA%20GCBA%20SOBRE%20AMPARO%20-OTROS.%207.9.2022.pdf

214/ Nota Técnica No. 175/2023 CGF/ANPD. "Acordo de Cooperação MJSP e CBF." Agência Nacional de Proteção de Dados, 2023. Punto 5.119. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf

ción de Datos (AEPD) concluyó que esta medida no es jurídicamente viable ni cumple con el RGPD.[215]

Por regla general, el tratamiento de datos biométricos está prohibido en la Unión Europea, a menos que el tratamiento sea necesario para atender un interés público esencial. Sin embargo, para el Tribunal Constitucional de España no es suficiente que exista una causa de interés público para permitir el tratamiento de datos biométricos. Este tratamiento también debe estar previsto en una ley que establezca las reglas precisas y garantías adecuadas para prevenir riesgos, y cumplir con el principio de proporcionalidad.

Pese al rechazo de la AEPD a este proyecto, LaLiga inició la licitación para contratar un sistema para el acceso a los estadios. La AEPD dirigió una advertencia a LaLiga donde alertó nuevamente sobre el riesgo y determinó que, previo a cualquier decisión sobre la implementación de un sistema que implique el tratamiento de datos biométricos, debe cumplir con ciertos requisitos, como presentar y superar favorablemente una EIP (evaluación de impacto en la privacidad). La AEPD señaló que en caso de no adoptar esas medidas, LaLiga podría incurrir en una infracción que desemboque investigaciones y sanciones.[216]

Como podemos ver, existe una tendencia alrededor del mundo de presentar a las TRF como la solución que garantizará la seguridad en los estadios. No obstante, en los países donde estos sistemas han sido evaluados por autoridades judiciales y administrativas, han sido considerados ilegales y objetos de alerta por las implicaciones que tiene para la privacidad, la protección de datos personales y otros derechos humanos.

FAN ID EN MÉXICO: UN SISTEMA OPACO E INEFICIENTE

Como respuesta a la violencia del Estadio Corregidora en marzo de 2022, Mikel Arriola, presidente de la Liga MX, anunció la implementación del sistema Fan ID: un sistema de reconocimiento facial obligatorio para toda la afición que busca identificar a quienes generen disturbios en los estadios. Este sistema implicaría la inversión de más 250 millones de pesos y se implementaría gradualmente hasta estar presente en todas las ligas mexicanas.[217]

Este sistema funciona mediante un sitio web, en el cual la persona debe ingresar una serie de datos personales, una foto de su credencial de elector (INE) y una foto de su cara (*selfie*). Este registro genera un código QR que la persona debe mostrar al momento de ingresar al estadio. En el estadio, el personal escanea dicho código y toma nuevamente una fotografía del rostro de la persona para que el sistema autorice o niegue el ingreso.

//* ----------

215/ Agencia Española de Protección de Datos. Informe 2022-0098. Agencia Española de Protección de Datos, 2022. Página 15. https://www.aepd.es/documento/2022-0098.pdf

216/ Agencia Española de Protección de Datos, Advertencia AI-00394-2023. 2023. 6. https://www.aepd.es/documento/ai-00394-2023-advertencia.pdf

217/ Liga MX: Fan ID con Poco Uso Después de la Tragedia en Querétaro." ESPN, 17 de agosto de 2023. https://www.espn.com.mx/futbol/mexico/nota/_/id/13524560/liga-mx-fan-id-poco-uso-despues-de-tragedia-queretaro

< Imagen de @LigaBBVAMX />

En los primeros anuncios sobre el Fan ID, Arriola informó que quien no diera su identidad sería "descartado" para ingresar a los partidos de fútbol.[218] Además, señaló que los estadios tendrían la obligación de habilitar sistemas de vigilancia con reconocimiento facial adentro de sus instalaciones. Los datos obtenidos del Fan ID –según afirmó– se compartirían con Plataforma México[219]; la red nacional de bases de datos criminalísticas a cargo de la Secretaría de Seguridad Pública y Protección Ciudadana (SSPC).

Las declaraciones por parte de las entidades futbolísticas generaron duda y polémica respecto a si esta solución carente de un análisis previo sería efectiva para evitar la repetición de sucesos como el del Corregidora, ya que las implicaciones del Fan ID para los derechos humanos ponen en riesgo las personas que asisten a los estadios, y es necesario garantizar que la solución no genere más daños que los ya causados. Desde R3D expresamos estas preocupaciones desde los primeros anuncios del Fan ID,[220] tanto pública como directamente ante la FMF y el INAI, y pedimos que incluyeran a la sociedad civil en el análisis de esta herramienta.[221]

//* ----------

218/ TUDN MEX (@TUDNMEX). X, 13 de marzo de 2022. https://x.com/TUDNMEX/status/1502808491639115780

219/ González Villalba, Héctor. Milenio. Liga MX se conectará a Plataforma México para enviar datos y rostros de delincuentes. 13 de marzo de 2022. https://www.milenio.com/futbol/liga-mx/liga-mx-conectara-plataforma-mexico-frenar-violencia

220/ R3D. "FMF y Liga MX Imponen Medidas Autoritarias y Demagógicas que Ponen en Riesgo a la Afición." R3D, 16 de marzo de 2022. https://r3d.mx/2022/03/16/fmf-y-liga-mx-imponen-medidas-autoritarias-y-demagogicas-que-ponen-en-riesgo-a-la-aficion/

221/ R3D (@R3Dmx). X, 4 de abril de 2022. https://x.com/R3Dmx/status/1511114495904698381

Sin embargo, en abril de 2022 el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y la FMF instalaron una mesa de trabajo a puerta cerrada para hablar sobre el Fan ID.[222] Después, en junio de dicho año, la FMF presentó una Evaluación de Impacto en la Protección de Datos Personales (EIP) para obtener la validación de este sistema por parte del INAI.

Cabe mencionar que, previamente, el INAI había sancionado a la FMF por una multa de 23 millones de pesos, según información consultada por Fox Sports. La razón de esta sanción fue el recabo de datos personales, incluidos los de menores de edad, de quienes acudieron a los partidos de la selección mexicana en el Estadio Azteca a inicios de 2022.[223] Esto significa que la FMF registró personas aficionadas incluso antes de la tragedia del Corregidora, sin haber hecho consulta alguna al INAI.

Al momento de la elaboración de este informe, las EIP no tienen un fundamento en las leyes mexicanas, por lo que no existen estándares definidos para presentarlas, ni facultad del INAI para obligar a la FMF a cumplir con sus determinaciones sobre estas evaluaciones. De esta forma, en agosto de 2022 el INAI emitió una Opinión técnica con recomendaciones sobre el Fan ID, las cuales la FMF podía decidir si seguir o no.[224]

El siguiente análisis está basado en información obtenida de solicitudes de acceso a la información presentadas por R3D y de la investigación y análisis de otras fuentes de información. La EIP elaborada por la FMF fue clasificada totalmente y la Opinión técnica emitida por el INAI fue clasificada en grandes porciones por razones de secreto industrial y comercial. El uso de la figura de secreto industrial para mantener en la opacidad la información sobre un sistema que afecta directamente derechos humanos aumentó las preocupaciones sobre el uso de esta herramienta en los estadios del fútbol mexicano.

Obligatoriedad de la medida

El solo tratamiento de datos pone en grave riesgo las libertades de las personas en una TRF. Sin embargo, que la medida sea impuesta como obligatoria hace ineludibles todos estos riesgos. La normativa de la FMF establece que, a partir de la temporada 2022-2023, todas las personas tendrán la obligación de registrarse en el Fan ID. Aunado a esto, señala que todos los estadios deben estar equipados en su interior y exterior con cámaras de

//* ----------

222/ Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). "INAI, FEDERACIÓN MEXICANA DE FÚTBOL Y LIGA MX INSTALARÁN MESA DE TRABAJO PARA ANALIZAR FAN ID Y GARANTIZAR PROTECCIÓN DE DATOS DE AFICIONADOS" INAI, 4 de abril 2022. https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-103-22.pdf

223/ Montes, J. INAI impone multa millonaria a Femexfut por campaña para registrar aficionados. 12 de enero de 2023. Fox Sports, 12 de enero 2023. https://www.foxsports.com.mx/2023/01/12/inai-impone-multa-millonaria-a-femexfut-por-campana-para-registrar-aficionados/

224/ Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). "INAI, FEDERACIÓN MEXICANA DE FÚTBOL Y LIGA MX INSTALARÁN MESA DE TRABAJO PARA ANALIZAR FAN ID Y GARANTIZAR PROTECCIÓN DE DATOS DE AFICIONADOS." INAI, 17 de agosto de 2022. https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-248-22.pdf

circuito cerrado de televisión (CCTV) para tomar fotografías individuales dentro y fuera del estadio.

Las imágenes obtenidas con estas cámaras deben ser compartidas con las autoridades de seguridad pública a través del Centro de Comando C2 y/o C5. El Fan ID crea una lista de personas bloqueadas, la cuales incluirán a las personas vetadas a solicitud de las autoridades por antecedentes de violencia.

> Los datos obtenidos por el Fan ID son utilizados para desarrollar y mejorar los algoritmos del proveedor, así como comprender patrones de uso, comportamientos y preferencias del usuario. Esto se traduce en prácticas de perfilamiento.

Tratamiento de datos

Incode Technologies es la proveedora de la TRF del Fan ID, la cual ofrece servicios de identificación y autenticación de identidad basada en inteligencia artificial.[225] En palabras del CEO de Incode, Ricardo Amper, la tecnología implementada en el Fan ID es la misma que se utiliza para "proteger tu identidad en bancos, en un aeropuerto o para poder votar en otros países".[226] Esto genera dudas sobre la explotación indebida de los datos obtenidos.

El INAI señaló en su Opinión técnica que el tratamiento de datos del Fan ID implica un alto riesgo por la gran escala de datos sensibles obtenidos en todo el país, el tratamiento de datos de menores de edad, las posibles prácticas de perfilamiento, los riesgos de vigilancia permanente, el impacto de los sesgos, la potencial discriminación y las consecuencias irrevocables que podrían surgir de la vulneración de este gran número de datos personales.[227]

La FMF informó en su EIP que el Fan ID funciona con tecnología 1:1; es decir, el sistema busca verificar si la foto de la credencial del INE del titular y su selfie coinciden, sin que el sistema busque empates del rostro con otras bases de datos. Sin embargo, el INAI alerta que el sistema utilizará tecnología 1:N para detectar a las personas de forma individual en la entrada y dentro de una multitud, lo que implica que sí se busca la *selfie* dentro de una base de datos. Por tanto, el rostro podría buscarse en cualquier base –como declaró Mikel Arriola en un inicio, respecto a la Plataforma México– o cualquier otra en manos de Incode y/o de entidades de gobierno.

Existen dos avisos de privacidad disponibles para el Fan ID: uno de la FMF y otro de Incode. Estos documentos indican que la persona debe registrar su nombre completo, datos de contacto, identificación oficial, foto del rostro, plantilla biométrica, así como datos para obtener

//* ----------

225/ Opinión técnica sobre la Evaluación de Impacto en la Protección de Datos Personales, emitida por el INAI, p. 24.

226/ El Universal Deportes. Presentan el FAN ID de la Liga MX- Mikel Arriola explica todos los detalles. 17 de noviembre 2022. https://www.youtube.com/watch?v=vgqhkB4dqIs. Min. 5:44.

227/ Opinión técnica sobre la Evaluación de Impacto en la Protección de Datos Personales, emitida por el INAI, 114, 115, 116, 117, 50, 107, 108, 109, 119.

información de la cuenta y actividad. Menores de edad de entre 15 y 17 años deben subir también una *selfie*, y datos de su titular para poder entrar a los estadios.

El aviso de privacidad de la FMF indica que no trata biométricos, ya que el tratamiento de dichos datos lo hace Incode. Sin embargo, esto no queda del otro claro ya que dentro de la lista de datos personales que obtienen se contemplan los biométricos, tanto para personas adultas como para menores de edad.[228]

Igualmente, señala que los datos serán compartidos con autoridades de seguridad pública, fiscalías y organismos judiciales sin necesidad de obtener el consentimiento previo. Al ser esta medida obligatoria y no opcional, no existe posibilidad de persona de elegir si su información personal es compartida y/o utilizada por autoridades públicas ni es posible impedir que a los datos de menores de edad sean compartidos también.

Por otro lado, el aviso de privacidad de Incode sí reconoce el tratamiento de datos biométricos, además de otros como geolocalización, dirección IP y modelo de dispositivo para conocer la actividad del titular.[229] Entre los objetivos para obtener los datos personales, está: *el desarrollo y mejora de sus algoritmos, así como la comprensión de patrones de uso, comportamientos y preferencias del usuario*. Esto implica la explotación de datos –tanto en esta tecnología como en otras que el proveedor desarrolle– para prácticas de perfilamiento que puedan resultar en discriminación.

Según los avisos de privacidad, no se transferirán datos biométricos. Sin embargo, las transferencias previstas en el aviso de Incode incluyen a terceros que contraten sus servicios, así como a las autoridades competentes, sin necesidad de obtener el consentimiento de la persona. La falta claridad sobre en manos de quién estarán estos datos puede expandir su explotación y aumenta las preocupaciones expuestas.

Transferencias de datos a autoridades

Junto con el anuncio del Fan ID como la solución a los problemas de violencia, las instituciones futbolísticas señalaron que esta TRF estaría conectada con Plataforma México (PM), la red de bases de datos criminalísticas a cargo de la SSPC. Entre la posterior negación de que existirían estos empates y la falta de información que demuestre esta información, aunado a la transferencia de datos a “autoridades competentes” establecida en los avisos de privacidad del Fan ID, existe incertidumbre sobre esta cuestión.

En diciembre de 2022, la SSPC anunció que había tenido reuniones con la FMF y con la Liga MX en las que hablaron del programa Fan ID. El entonces subsecretario de la SSPC, Ricardo Mejía, señaló que habían “establecido un mecanismo de identificación única de aficionados para que, en caso de violencia o en caso de un incidente, se pueda ubicar, de manera inme-

//* ----------

228/ Aviso de Privacidad Integral de la FMF para el Fan ID, vigente a agosto de 2024. Noviembre 2022. https://fanliga.mx/en/fmfPrivacy/

229/ Aviso de Privacidad de Incode Technologies para el Fan ID, vigente a agosto de 2024. Noviembre 2022. https://fanliga.mx/en/privacy

diata a la persona que está generando este tipo de incidentes",[230] lo cual podría incluir la conexión con PM y otras bases de datos de autoridades de seguridad.

Pese a esto, en solicitudes de acceso a la información promovidas por medios de comunicación para conocer estos acuerdos, la SSPC negó tenerlos. Ante esto, en septiembre de 2023, el INAI determinó que las declaraciones públicas de la SSPC demostraban que la información tenía que existir y ordenó que la dependencia informara debidamente sobre estos acuerdos y que diera la lista de estadios y equipos conectados a la PM, la fecha en que ingresaron y las detenciones logradas.[231]

Aun con lo ordenado por el INAI, ni la SSPC ni la FMF se han pronunciado al respecto, por lo que no existen registros que informen formalmente que las transferencias de datos con PM se hayan cancelado o que no se hayan iniciado.

Además de estas colaboraciones, la Secretaría de Seguridad Ciudadana de la Ciudad de México se ha coordinado previamente con la FMF y la Liga MX. Por ejemplo, en la firma de un convenio de colaboración "para fomentar el orden y la convivencia pacífica para erradicar distintos tipos de violencia, incluyendo el acoso digital". En la consolidación de este acuerdo no dejó de estar presente la mención del Fan ID como la herramienta que "indudablemente ha atendido la violencia en los estadios".

Pese a la implementación del Fan ID, a un mes de terminar el torneo Clausura 2023 se presentaron al menos 10 sucesos violentos. A poco más de la mitad del torneo Clausura 2024, se identificaron 25 incidentes.

La falta de efectividad del Fan ID

Según datos oficiales de la Liga MX, a marzo de 2024, el torneo Apertura 2023 tuvo una asistencia de 3.07 millones de asistentes. Esta cifra representó un incremento del 158% en la asistencia a los partidos. Se credencializaron a más de 18 mil 500 miembros de grupos de animación que pueden ingresar a sus estadios locales, mientras que se prohibió el ingreso a grupos de animación visitantes.

Los datos de la Liga MX señalan que, hasta ese momento, se contaban con poco más de dos millones 100 mil registros, y que "se han bloqueado a 30 aficionados por conductas violentas y los escaneos han aumentado su efectividad pasando de 25% a 42% del torneo Clausura al Apertura 2023".[232]

//* ----------

230/ Secretaría de Seguridad y Protección Ciudadana. SSPC, FMF y Liga MX coordinan acciones para mejorar prácticas deportivas y seguridad en el fútbol. 9 de diciembre 2022. https://www.youtube.com/watch?v=wuFopOeCi50

231/ INAI. SSPC DEBE DAR A CONOCER ESTADIOS Y EQUIPOS DE LIGA MX CONECTADOS A PLATAFORMA MÉXICO, PARA REDUCIR VIOLENCIA EN PARTIDOS. 9 de septiembre 2023. https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-070-23.pdf

232/ Arriola, Mikel (@MikelArriolaP). X, 5 marzo de 2024. https://x.com/MikelArriolaP/status/1765115223009063412

En distintas declaraciones, Mikel Arriola ha asegurado que esta medida ha sido útil para erradicar la violencia en los partidos, señalando que tras lo sucedido en el Estadio Corregidora "la acción más importante [ha sido] la implementación del Fan ID. El principal problema es el anonimato y este sistema de credencialización permite atacar el motivo de violencia en las canchas".[233]

Pese a la implementación del Fan ID, entre 2022 y 2024 se han reportado diversos incidentes de violencia. Información de ESPN indica que, a un mes de terminar el torneo Clausura 2023, se presentaron al menos 10 sucesos violentos.[234] A poco más de la mitad del torneo Clausura 2024, reporteros lograron identificar 25 incidentes, incluyendo el atropello de una aficionada que perdió la vida, el accidente más grave en dicho torneo.[235]

< Imagen de Pasión Águila />

ESPN señaló que el Fan ID se ha pedido de manera aleatoria para entrar a los estadios en un porcentaje no mayor a 1 de cada 5 aficionados.[236] Diferentes periodistas y personas de la afición han coincidido con estos datos al señalar que "[han] visto en muchas ocasiones que nada más revisan dos o tres aficionados y a los demás los dejan pasar sin hacer el escaneo

//* ----------

233/ Schiller, Nicolás. El Universal. A un año de la tragedia, sólo llegó el Fan Id. 5 de marzo de 2023. https://www.eluniversal.com.mx/universal-deportes/liga-mx-un-ano-de-la-tragedia-en-queretaro-solo-llego-el-fan-id/

234/ Liga MX: Recuento de incidentes de violencia en el Clausura 2023." ESPN, 26 de abril de 2023. https://www.espn.com.mx/futbol/mexico/nota/_/id/11958553/liga-mx-recuento-de-incidentes-de-violencia-en-el-clausura-2023

235/ Lecanda, León. "Liga MX: El poco uso del Fan ID después de la tragedia en Querétaro." ESPN, 16 de abril de 2024. https://www.espn.com.ar/futbol/mexico/nota/_/id/13524560/liga-mx-fan-id-poco-uso-despues-de-tragedia-queretaro

236/ *Idem*.

del Fan ID porque muchas veces está cerca de arrancar el partido y (...) la seguridad los deja pasar para evitar que haya problemas de los aficionados que están molestos".[237]

Además, se ha reportado en redes sociales que esta medida ha sido frecuentemente burlada en los partidos. Según señalan, los bloqueos de ingreso a personas por antecedentes violentos son una simulación porque no piden el Fan ID, o que únicamente piden el QR sin verificar que este código pertenece a quien lo porta para evitar aglomeraciones. Por otro lado, testimonios informan que cuando el Fan ID de una persona está bloqueado, afuera del Estadio Azteca "por 50 pesos te expedían un Fan ID sin tener que dar tus datos" e incluso señalan que aficionados con veto han logrado entrar a los estadios de esta manera.

El sistema Fan ID ha sido deficiente, ya que no ha logrado abordar adecuadamente los problemas que motivaron su implementación. No ha logrado evitar la violencia e incluso ha sido preferible no usarlo en las entradas para evitar aglomeraciones que causen más violencia. Al poder ser burlada, esta medida no garantiza la seguridad deseada. A pesar de su infectividad, el Fan ID ya ha recopilado los datos de millones de personas y los derechos humanos de quienes asisten a los estadios están siendo vulnerados a cambio de un sistema que no soluciona los problemas que buscaba resolver.

"En muchas ocasiones, nada más revisan dos o tres aficionados y a los demás los dejan pasar sin hacer el escaneo del Fan ID porque está cerca de arrancar el partido. La seguridad los deja pasar para evitar que haya problemas de los aficionados que están molestos" - Juan Dávalos, reportero.

¿CÓMO AFECTA NUESTROS DERECHOS LA TRF EN ESTADIOS?

Privacidad y protección de datos personales

La TRF en estadios viola la privacidad y la protección de datos de toda persona que busca entrar a estos recintos. La obtención de datos personales como el domicilio (obtenido de la identificación oficial), edad, contacto, datos del dispositivo (dado que el registro es mediante el celular) y biométricos (rostro), tanto para adultos como para menores de edad, es desproporcionada e invasiva.

La ley exige que las personas den su consentimiento expreso para que terceros puedan tratar sus datos personales. A pesar de esto, para entrar a los estadios el consentimiento expreso se vuelve una simulación. En realidad, las personas no pueden negarse a que sus datos sean tratados, por ejemplo, para ser transferidos a autoridades que podrán disponer de ellos a su conveniencia, o a que sus datos sean utilizados para entrenar otros modelos algorítmicos que serán implementados en otros contextos. De esta forma, los datos de la persona podrían terminar, sin su conocimiento, en múltiples bases de datos sin que exista un mecanismo real para negarse.

//* ----------

237/ La Octava Sports. EN VIVO | EL FAN ID, EL GRAN MITO DE LA LIGA MX. 26 de enero 2024. https://www.youtube.com/watch?v=a4yRqeeOJ00

El simple hecho de que existan bases con datos sensibles de las personas también vulnera estos derechos por las consecuencias graves que pueden surgir en caso de que estas bases sean vulneradas o filtradas. Si bien una filtración de datos de contacto o el domicilio de una persona puede ser riesgoso, la vulneración de una base con caras y otros –varios– datos, como en el caso de las TRF en estadios, puede generar afectaciones irreparables. Esto es aún más preocupante en casos como el de Brasil, donde se propuso conservar las bases de datos por 50 años, lo cual fomenta la vigilancia estatal injustificada de personas que no son buscadas por las autoridades.

Las TRF habilitan prácticas de perfilamiento que clasifican a las personas conforme a gustos, patrones, preferencias, características físicas, edad, situación social, entre otras cuestiones. En el contexto deportivo o artístico, estas preferencias son fácilmente categorizables, lo cual permite generar bases que realicen perfilamiento de grupos históricamente oprimidos.

Por ejemplo, si el sistema tiene determinado que los hinchas varones de cierto equipo –con la tez de cierto tono y la cara de cierta forma– son tendenciosas a ser violentos, probablemente le nieguen la entrada al aficionado que entre en esas categorías, o bien, cualquier persona que cumpla con las mismas sea detenida, ya sea por un resultado erróneo o porque exista un perfilamiento racial en su contra.

Libertad de expresión y reunión pacífica

Las violaciones a los derechos a la privacidad y protección de datos conlleva la violación de la libertad de expresión. Ser una persona identificada con TRF en los estadios implica no poder disfrutar de estos eventos, ya sea con una expectativa de privacidad o en el total anonimato, lo cual puede generar un efecto intimidatorio que impida la libertad de expresión de quienes asisten a esos eventos.

Las preferencias por ciertos equipos, la manifestación de pensamientos y emociones, la manera de vestirse y las conexiones con personas con preferencias similares son algunas formas de expresión en contextos deportivos y artísticos. Estas expresiones se pueden ver disminuidas por miedo a ser objeto de actos arbitrarios originados por el tratamiento masivo de datos. Estos actos comprenden posibles identificaciones erróneas basadas en el perfilamiento de personas. Una práctica de perfilamiento que afectaría la libertad de expresión es el establecimiento de suposiciones o estereotipos trasladados a una TRF.

Un ejemplo de esto sería “los hinchas varones de tal equipo de entre 20-30 años, con tez de cierto tono y rasgos con ciertas características, son más propensos a ser violentos”, lo cual generaliza negativamente a ciertos grupos y genera consecuencias para toda persona que cumpla con estas características. La posibilidad de ser objeto de actos arbitrarios, injusticias e incluso detenciones por cumplir con ciertas particularidades, derivado de resultados de algoritmos sesgados, cambian la manera en la que una persona se expresa y afecta la libertad de expresión.

Incluso, los TRF pueden inhibir la libertad de expresión fuera de los estadios. Al ser utilizadas para negar la entrada a opositores del gobierno, como en Rusia, o para vetar a quienes son considerados “enemigos” de los dueños de los recintos, como en Estados Unidos, estas tec-

nologías generan un efecto intimidatorio que limita la libertad de expresión en otros ámbitos, ya que puede disuadir a las personas de expresar opiniones críticas por temor a represalias.

Igualdad y no discriminación

Los sesgos trasladados a las TRF, las prácticas de perfilamiento y las tasas de error de los sistemas con TRF arrojan resultados que impactan negativamente a grupos en situación de vulnerabilidad, como personas de color, personas indígenas, mujeres o personas de la comunidad LGBTTTIQ+. El impedimento a ejercer derechos humanos por cumplir con ciertas características físicas es discriminatorio y, como hemos reiterado, puede hacer a las personas que cumplan con las mismas sean víctimas de distintos actos arbitrarios.

Por ejemplo, en el Mundial de Catar 2022, la TRF "predecía" los patrones de las multitudes, lo cual ayudó a identificar e intimidar a personas que utilizaban la bandera de la comunidad LGBTTTIQ+. En Gales del Sur, la policía desconocía el conjunto de datos con el que se había "entrenado" la tecnología, por lo que no podía saber si había un equilibrio demográfico en los datos usados para entrenar el algoritmo. Estas posibles subrepresentaciones generan resultados que desfavorecen a los grupos en situación de vulnerabilidad.

< Imagen de Tembhela Bohle />

Acceso a la cultura

Los espectáculos deportivos y musicales constituyen espacios que pertenecen a la vida cultural de México. La participación de las personas en estas actividades no solo contribuye al desarrollo de su identidad, sino que genera un sentimiento de pertenencia y comunidad que son parte esencial de su participación en la vida cultural.

El derecho a la cultura engloba el derecho de acceso a la cultura, el derecho de paricipar a la vida cultural y contribuir a la cultura. El Comité de Derechos Económicos, Sociales y Culturales, en su observación General No. 21,[238] establece que la participación en la vida cultural comprende:

> El derecho de toda persona (sola, en asociación con otras o como una comunidad) a actuar libremente; a escoger su propia identidad; a identificarse o no con una o con varias comunidades, o a cambiar de idea; a participar en la vida política de la sociedad; a ejercer sus propias prácticas culturales y a expresarse en la lengua de su elección.

El acceso a la cultura fomenta valores esenciales para la sociedad, como la comprensión, la flexibilidad y la tolerancia hacia otras culturas y perspectivas, lo cual promueve entornos más inclusivos y respetuosos. También comprende el derecho de toda persona a conocer y comprender su propia cultura y la de otros, a través de la educación y la información, y a recibir educación y capacitación de calidad con pleno respeto a su identidad cultural. Igualmente, incluye:

> Conocer formas de expresión y difusión por cualquier medio tecnológico de información y comunicación; a seguir un estilo de vida asociado al uso de bienes culturales y de recursos como la tierra, el agua, la biodiversidad, el lenguaje o instituciones específicas, y a beneficiarse del patrimonio cultural y de las creaciones de otros individuos y comunidades.

Con la implementación del FAN ID, el derecho de acceso a la cultura se ve condicionado a la obligación de un registro biométrico que puede negar la entrada de las personas a los estadios a través de resultados sesgados o erróneos.

En México, según la empresa de estadística Nielsen, en 2019 el 73% de la población mexicana era aficionada del fútbol.[239] En 2023, la empresa YouGov informó que para el 20% de los

//* ----------

238/ Comité de Derechos Económicos, Sociales y Culturales. Observación general Nº 21. https://www.acnur.org/fileadmin/Documentos/BDL/2012/8793.pdf

239/ Record. Sexto País con el Mayor Número de Aficionados al Fútbol. 10 de junio 2019. https://www.record.com.mx/futbol-futbol-nacional-liga-mx-noticias/mexico-sexto-pais-con-el-mayor-numero-de-aficionados-al

mexicanos, asistir a eventos deportivos es una de sus actividades favoritas para disfrutar su tiempo libre.[240] Esta preferencia se refleja en la creciente asistencia a los estadios, que para el año 2024 culminó con 6.64 millones de aficionados.[241]

En este caso, la obligación de registrarse en el Fan ID condiciona el ejercicio del derecho de acceso a la cultura de prácticamente tres cuartas partes de la población mexicana. Aparte, obstaculizaría el acceso a este derecho a todas las personas a las que se les impide el acceso debido a sesgos y errores de la TRF o por pertenecer a la "lista negra" de la Federación Mexicana de Fútbol.

Un ejemplo de esto sería el bloqueo de las personas en condiciones de pobreza bajo el sesgo predeterminado de que "las personas que se encuentran en esta situación económica tienden a propiciar la inseguridad en los estadios". Esto resulta en la perpetuación de sesgos clasistas que suprimen el desarrollo de la vida cultural de comunidades enteras, y genera un efecto intimidatorio en las personas que logran acceder a los partidos por miedo a ser víctimas de estos bloqueos.

Presunción de inocencia

Las TRF en estadios violan la presunción de inocencia. La obligatoriedad de la medida –incluso para personas menores de edad, como en México– le da un trato de sospechosa a toda aquella que se registre en el sistema, independientemente de que esté siendo buscada por las autoridades o no.

La transferencia a autoridades de seguridad pública, como fue planteado en Brasil y sucede en Argentina y México, implica una vigilancia permanente por parte de los estadios y las autoridades de seguridad pública. De esta forma, asume que todos los individuos son culpables hasta que se demuestre lo contrario.

En el caso de Rusia, la TRF es utilizada para reprimir a críticos del gobierno y activistas. En Estados Unidos, como ya mencionamos, se negó la entrada a conciertos de las personas consideradas como "enemigas" del propietario de los estadios. Estas arbitrariedades demuestran la facilidad con la que los operadores de estos sistemas pueden asumir como culpable a cualquier persona de cualquier cosa, incluso de actividades que no se traten de un delito, sino de expresiones o actos incómodos para quienes operan estos sistemas o actores políticos.

//* ----------

240/ YouGov Research: ¿Cuáles Son los Deportes Más Populares del País? 16 de agosto de 2023. https://business.yougov.com/es/content/47576-mexico-cuales-deportes-mas-populares-pais

241/ Flores Aldana, D. Liga MX: ¿Hay crisis de asistencia de aficionados a los estadios? *ESPN Deportes*. 13 de noviembre de 2024. https://www.espn.com.mx/futbol/mexico/nota/_/id/14438454/liga-mx-asistencia-aficionados-estadios-apertura-2024-baja

"No tiene sentido someter los datos recogidos de ciudadanos que están ejerciendo plenamente sus derechos y no son objeto de actividades de seguridad pública a un tratamiento que llevaría a su conservación durante 50 años o más"- Autoridad Nacional de Protección de Datos, sobre la TRF en estadios de Brasil.

NECESIDAD DE ALTERNATIVAS

La Agencia Española de Protección de Datos ha indicado que la TRF en estadios no es la única forma de buscar la seguridad. Para la AEPD, estos sistemas:

> "[F]avorecen a la organización y no a los aficionados (...) y es que, cuando existan opciones realmente equivalentes y disponibles para todos los aficionados para acceder a los estadios de fútbol que resulten menos intrusivas para sus derechos y libertades, y permitan identificar-verificar la identidad de los aficionados, como puede ser la exhibición del título de acceso junto al documento acreditativo de su identidad, resulta difícilmente justificable la necesidad de implementar sistemas más intrusivos como los de tratamiento biométrico. (...) [En la implementación de reconocimiento facial] no cabe confundir necesidad con conveniencia de la organización."[242]

Existen alternativas menos intrusivas para las personas, el procesamiento de datos deja de ser necesario y justificable. El balance entre costo-beneficio del Fan ID en México no ha sido favorable. La persistencia de los problemas de violencia a pesar de la invasión a la privacidad y otros derechos humanos exige la necesidad de detener el uso de estos sistemas y buscar otras alternativas.

Podemos encontrar una alternativa al analizar el caso colombiano. En Colombia, el programa "Goles en Paz" ha abordado los problemas de violencia en las barras de Bogotá mediante el diálogo, la inclusión social y la resolución pacífica de conflictos. Según reportes de la Secretaría de Gobierno de Bogotá, durante el primer semestre de 2022, este programa logró la celebración de 109 partidos con más de 400 mil asistentes "en completa paz y calma".[243]

//* ----------

242/ Agencia Española de Protección de Datos, Advertencia AI-00394-2023. 2023. 6. https://www.aepd.es/documento/ai-00394-2023-advertencia.pdf

243/ Landínez Cañón, D. En más de 100 partidos ¡Goles en paz 2.0 la ha dado al cien!. Alcaldía de Bogotá. 11 de septiembre 2022. https://bogota.gov.co/mi-ciudad/gobierno/mas-de-100-partidos-este-ano-avanza-de-forma-segura-goles-en-paz-20

Goles en Paz organiza diversas actividades deportivas, talleres educativos, espacios de diálogo con diferentes actores, acompañamientos a barras y apoyo en partidos.[244] La detección de diferentes necesidades ha inspirado diferentes campañas dentro de este programa, como las dirigidas a las infancias con el fin de que aprendan sobre una cultura de sana convivencia en el fútbol. También ha incluido la campaña "Aguante, fiesta y fútbol", la cual apoya la instalación de carpas afuera de los estadios para habilitar vendimias y otras actividades comerciales para apoyar a las familias de Bogotá.

Otra campaña dentro de este programa es "Aguante femenino la misma pasión", la cual visibiliza y reconoce a las mujeres en el fútbol mediante el uso simbólico de paliacates o bandanas. El involucramiento de las barras con las instituciones de "Goles en Paz" también ha llevado a la creación de la Ley 1270,[245] la cual crea la Comisión Nacional de Seguridad, Comodidad y Convivencia en el Fútbol y reconoce a todos los actores para garantizar la seguridad en el fútbol. Contempla la adopción de protocolos, logísticas y medidas para mejorar la seguridad en los partidos.

Bogotá ha reconocido al fútbol como una fuente de recreación y cultura que afecta diferentes dimensiones de la sociedad, y la escucha activa de las necesidades de las barras y las personas aficionadas ha logrado abordar las problemáticas de violencia. No solamente desde la logística en los partidos, sino desde un enfoque preventivo que busca atender a todos los sectores para crear una cultura pacífica y tolerante en el fútbol.

El caso de Bogotá ejemplifica la necesidad de buscar estrategias que vayan más allá de la adquisición de tecnología y se enfoquen en alternativas que prioricen el análisis de los componentes sociales y culturales que provocan la violencia en el deporte. Los tomadores de decisiones en el fútbol deben reconocer a este deporte como un catalizador de cultura, y a las barras y la afición como un agente que lo moviliza, sin dejar de lado a los actores que suelen ser excluidos, como las mujeres, las infancias y la juventud.

Contrario a lo anterior, en México se presentó el Fan ID como la solución que "indudablemente" resolvería los problemas de violencia. Sin embargo, este proyecto buscar atender posibles eventos violentos después de que sucedieron, sin un análisis previo de la pertinencia y proporcionalidad de este sistema.

No se incluyó a las partes involucradas en el fútbol ni a la sociedad civil, por lo que no existió la posibilidad de buscar otras alternativas que pudieran ser menos intrusivas para los derechos de la afición. Mientras los esfuerzos por enfrentar la violencia busquen solamente encontrar a las personas culpables y no aborden el problema de manera preventiva –es decir, evitar que la violencia suceda en primer lugar– su funcionamiento será poco factible.

//* ----------

244/ Fierro, C. Goles en paz ha reforzado la convivencia en 459 partidos de fútbol este 2023. Alcaldía de Bogotá. 13 de julio 2023. https://bogota.gov.co/mi-ciudad/gobierno/en-1er-semestre-de-2023-se-impusieron-17-comparendos-hinchas

245/ Ley 1270 de 2009 que crea la Comisión Nacional para la Seguridad, Comodidad y Convivencia en el Fútbol y otras disposiciones. Congreso de Colombia. Publicada en el D.Ol 47.223 de enero 5 de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34491#:~:text=Cr%C3%A9ase%20la%20Comisi%C3%B3n%20Nacional%20de,organizaci%C3%B3n%20y%20pr%C3%A1ctica%20de%20este

¿Qué sucede con las barras y la afición en México? ¿Se les da el reconocimiento necesario? ¿Qué significa el fútbol para las y los mexicanos? ¿Qué elementos originan la violencia? ¿Cómo pueden trabajar en conjunto todos los actores del fútbol para garantizar un entorno seguro y respetuoso para toda la afición? Son algunas de las preguntas que los tomadores de decisiones de fútbol podrían empezar a hacer.

CONTRA LA NORMALIZACIÓN DE LA TRF EN LOS ESTADIOS

Como desarrollamos en este apartado, existe una tendencia alrededor del mundo de presentar a las TRF como la solución que garantizará la seguridad en los estadios. No obstante, en los países donde estos sistemas han sido evaluados por autoridades judiciales y administrativas, esta TRF ha sido considerada ilegal y objeto de alerta por las implicaciones que tiene para la privacidad, la protección de datos personales y otros derechos humanos.

El Fan ID en México ha sacrificado los derechos de las personas que asisten a los estadios a cambio de un proyecto que no ha solucionado los problemas de violencia. A pesar de su operación deficiente, este sistema ya ha obtenido los datos de más de 2 millones de personas, los cuales incrementan en cada partido que es solicitado, sin que exista certeza sobre qué hacen con esos datos y con quién los comparten.

Este proyecto ha sido problemático desde su concepción, y la opacidad y las irregularidades respecto a este sistema han incrementado nuestras preocupaciones. Son diversas las causas que generan estas inquietudes: la falta de transparencia sobre la EIP; la convicción que lo asumía como la solución; la opacidad y falta de explicabilidad sobre su funcionamiento; el uso de figuras jurídicas para entorpecer la transparencia (como el secreto industrial); la imposición del registro obligatorio; las irregularidades en materia de protección de datos; las implicaciones graves para los derechos humanos; la falta de evaluaciones de impacto en los derechos humanos afectados; la falta de certeza sobre en qué manos caerán los datos; e incluso, la información que apunta que los datos de personas aficionadas fueron registradas antes de cualquier tipo de evaluación en partidos de la selección mexicana.

La normalización de espacios públicos hipervigilados mediante una TRF –que cuesta millones de pesos bajo la excusa de seguridad– coloca a las personas en estado de indefensión. ¿Cuáles son las verdaderas intenciones de la implementación del uso de TRF? Si las TRF que adquieren no están solucionando los problemas, ¿quién termina ganando?

La falta de efectividad en el caso de México y el rechazo de la TRF por parte de las autoridades de otros países nos lleva a pensar en alternativas, y en la necesidad de dejar de lado perspectivas tecnosolucionistas y encontrar la verdadera raíz del problema mediante enfoques sociales y culturales. A pesar de esto, la tendencia de implementar tecnología como una solución a los problemas de seguridad y violencia continúa, como en los Juegos Olímpicos de París 2024,[246]

//* ----------

246/ R3D. Francia implementará videovigilancia asistida por inteligencia artificial en París 2024. 11 de junio de 2024. https://r3d.mx/2024/06/11/francia-implementara-videovigilancia-asistida-por-inteligencia-artificial-en-paris-2024/

el registro de hinchas en Chile,[247] o el mundial de México, Estados Unidos y Canadá en 2026.[248] En un ecosistema donde nuestros datos pueden ser explotados, los sistemas pueden operar entre sí y son implementados en medio de irregularidades, ¿qué tan vulnerables nos encontramos? Nuestros derechos no deben formar parte de este juego.

//* ----------

247/ ANFP Chile. Registro Nacional de Hinchas suma 120 mil inscritos. 15 de abril de 2024. https://www.registrodelhincha.cl/

248/ TISA. Innovations That Shape the World Cup: 2022-2026. 17 de enero de 2023. https://www.tisagroup.ch/innovations-that-shape-the-world-cup/

CONCLUSIONES: NO NOS VEAN LA CARA

El principal objetivo de este informe es hacer un diagnóstico sobre la situación actual de la vigilancia con sistemas de TRF en México. Nos hemos enfocado en mapear las situaciones más urgentes que hemos documentado a lo largo de los años, no obstante, no son las únicas.

Los gobiernos estatales y el gobierno federal están cada vez más proponiendo las TRFs como soluciones a la seguridad pública. Igualmente, existen empresas privadas o particulares que imponen sistemas de identificación biométrica para cuestiones cotidianas como entrar a los edificios donde las personas trabajan o viven. La proliferación de este tipo de herramientas está fuera de control en un contexto donde existen pocas herramientas para hacer valer nuestros derechos.

La tecnología con capacidad de reconocimiento facial afecta gravemente los derechos humanos de todas las personas. El reconocimiento facial en espacios públicos implica daños inherentes. Es urgente que la población y las personas tomadoras de decisiones cuestionen las narrativas que existen alrededor de estas tecnologías. No podemos permitir que nos orillen a intercambiar nuestras libertades por falsas promesas de seguridad o soluciones a problemas que no existen.

Además, una TRF con registro biométrico obligatorio –sin que exista un verdadero consentimiento, como en el caso de los aeropuertos o los estadios– hace inevitables estos daños; y sus consecuencias, muchas veces, irreparables. Estas aseveraciones han sido ampliamente documentadas por diversas organizaciones defensoras de derechos humanos, académicas e incluso diversos tribunales alrededor del mundo. Nuestra democracia y la defensa de los derechos humanos no pueden permitirse podemos seguir ignorando estas evidencias.

Por lo tanto, realizamos las siguientes recomendaciones:

01// Es vital que podamos comprender cómo funcionan los sistemas con TRF. Para esto, se debe asegurar la máxima transparencia en cada una de las partes del ciclo de vida del software con capacidad de reconocimiento facial, desde que se desarrolla el modelo hasta su implementación y evaluación.

02// Es necesario que las autoridades estatales rindan cuentas sobre el uso de TRF en distintos espacios públicos. Esto incluye que den información relacionada con el tipo de tecnología que están usando, los proveedores, las tasas de error, las evaluaciones y pruebas que se han realizado a esos sistemas, entre otros.

03// Cualquier iniciativa que proponga el uso de TRF debe de estar acompañada de una evaluación exhaustiva de impacto a los derechos humanos. El derecho a la privacidad no es el único derecho afectado por esta tecnología. Por lo tanto, las evaluaciones de impacto deben de considerar derechos como la libertad de expresión, derecho a la no discriminación, presunción de inocencia, reunión pacífica, entre otros.

04// Las evaluaciones de impacto a los derechos humanos de las TRF deben de ser transparentes y abiertas a la participación ciudadana. El uso de la TRF en las calles es de interés público, por lo que la ciudadanía debe de tener conocimiento pleno de estas evaluaciones y poder aportar comentarios antes de que se implementen las TRF.

05// Las autoridades estatales deben de abstenerse de utilizar TRF sin que exista un marco legal claro y preciso que detalle el uso de este tipo de herramientas.

06// La política pública en materia de seguridad necesita alejarse del uso de bases de datos biométricas centralizadas. Los datos biométricos son datos sumamente sensibles y la vulneración de estos datos suponen daños irreparables.

07// De igual forma, las autoridades estatales deben evitar crear bases de datos biométricas con los marcos faciales que recolecten a través de la TRF. Estos datos tampoco deben de ser transferidos con otras autoridades o privados de manera opaca y encubierta.

08// La vigilancia masiva del espacio público realizada de manera remota inhibe la expresión libre. La vigilancia con TRF solo ha resultado en criminalización de personas manifestantes y el amedrentamiento de la expresión pública. Las autoridades estatales deben de abstenerse de utilizar TRF en espacios de protesta.

09// Es necesario establecer lineamientos para que las empresas y particulares que utilicen TRF en el espacio público realicen una evaluación de impacto a los derechos humanos, además de mecanismos de verificación para asegurarse de que estén cumpliendo con sus obligaciones en materia de protección de datos personales.

10// Las autoridades estatales deben de establecer una moratoria para el uso de TRF como herramienta para la persecución del delito. No existen las garantías seguridad suficientes que aseguren que una persona no pueda ser identificada erróneamente y sea acusada de un delito que no cometió. En general, el uso de TRF debe de limitarse lo más posible e, incluso, considerar dejar de utilizar TRF para la identificación biométrica por completo.

NO NOS VEAN LA CARA

VIGILANCIA EN EL ESPACIO PÚBLICO CON TECNOLOGÍAS DE RECONOCIMIENTO FACIAL EN MÉXICO

Escrito por: Francia Pietrasanta, Grecia Macías y Santiago Narváez

Editado por: José Flores

Portada e interiores: Gibrán Aquino

Mayo de 2025

```
((/(>(*!(*>(///*)(@)</)<<)*)))>))<!>(/<<)*/!/@!(/<(<///!*<*@**)>)(/<@>)/<!@()<!<!<@<*/!*(///)@/(@
//*)(!<@/<@<(@*(*@!/>!<)())<!!<*<)*((<)>@!*/!/**)!(/(*!)/!(@<>((/(>!<>@!@(*(>/!*>!!>>!!(<</<@/!>
(**)()!)(*(>()>@/(@)@/*!()*/<@<)/(*>((<@<//(@(//<!@<<*!>*(!((!*!/)()/@**/!<!@/(((*/(!</(>)(>//
>@))/(</>*(/>@/(<)*!<>*>@(*@*)*@!*)!@@>)@>**/>*!<<>/)(!)!)<@><<>!*)!(@!<(!)//<>)/(!)>><(@(@
/@)@<(><<!@(@*)<*<</()@(((@((@@>*(*!*!/((<((@/>!</@)!!>/()>>/<<<!)<(*/(!*!**)(>@>@()*))>/
/</(/*)<)(@!)(*)@/**/@//!>))<(/)!//))</@))))><(@@/(@!//!(>>>><<)>/*<>)@)**>)/@>!)/<!>!(*<**!@
/*)!@>(@>//!@(>)*(<>*(/)/((>*<<)@*/!*!(*(>><(!*<*!(*<@/>())/<@<</>!//!*<***@<>/@)>!/((>!/!@>>!
<@@<()@)<))(*/@>**(<*/*/!@**(>@*(>@)!**!*)>@))/(//!@()/!!)/*@<)!)@@/@*)@!>/)@/<!(><@
@*<<<)/)*<(<*(<@>*/@(>/>!)<<!()(>/>@!)<(!<*/@><<></)(<@!*!)<<!)>!/*!!/<!@)/>**)>!//)!<*/)//@!(<
)*<@>!</@*@)>(<((><!!!@)@))))>)(**/@*(!*<(/(/>!/*>!*)>!)*@/>>>)(>>**((/*!(@<!*<>@)//@>((/**!)@
@@/@)@<(><<!@(@*)<*<</()@(((@((@@>*(*!*!/((<((@/>!</@)!!>/()>>/<<<!)<(*/(!*!**)(>@>@()*)
(*/</(/*)<)(@!)(*)@/**/@//!>))<(/)!//))</@))))><(@@/(@!//!(>>>><<)>/*<>)@)**>)/@>!)/<!>!(*<**
/*)!@>(@>//!@(>)*(<>*(/)/((>*<<)@*/!*!(*(>><(!*<*!(*<@/>())/<@<</>!//!*<***@<>/@)>!/()(>!/!@>>
@!<@@<()@)<))(*/@>**(<*/*/!@**(>@*(>@)!**!*)>@))/(//!@()/!!)/*@<)!)@@/@*)@!>/)@/<!(><@
/<@*<<<)/)*<(<*(<@>*/@(>/>!)<<!()(>/>@!)<(!<*/@><<></)(<@!*!)<<!)>!/*!!/<!@)/>**)>!//)!<*/)//@!
!@)@>*<@>!</@*@)>(<((><!!!@)@))))>)(**/@*(!*<(/(/>!/*>!*)>!)*@/>>>)(>>**((/*!(@<!*<>@)//@>(
@@/@)@<(><<!@(@*)*<</()@(((@((@@>*(*!*!/((<((@/>!</@)!!>/()>>/<<<!)<(*/(!*!**)(>@>@()*)
(*/</(/*)<)(@!)(*)@/**/@//!>))<(/)!//))</@))))><(@@/(@!//!(>>>><<)>/*<>)@)**>)/@>!)/<!>!(*<**
/*)!@>(@>//!@(>)*(<>*(/)/((>*<<)@*/!*!(*(>><(!*<*!(*<@/>())/<@<</>!//!*<***@<>/@)>!/()(>!/!@>>
@!<@@<()@)<))(*/@>**(<*/*/!@**(>@*(>@)!**!*)>@))/(//!@()/!!)/*@<)!)@@/@*)@!>/)@/<!(><@
/<@*<<<)/)*<(<*(<@>*/@(>/>!)<<!()(>/>@!)<(!<*/@><<></)(<@!*!)<<!)>!/*!!/<!@)/>**)>!//)!<*/)//@!
!@)@>*<@>!</@*@)>(<((><!!!@)@))))>)(**/@*(!*<(/(/>!/*>!*)>!)*@/>>>)(>>**((/*!(@<!*<>@)//@>(
@@/@)@<(><<!@(@*)*<</()@(((@((@@>*(*!*!/((<((@/>!</@)!!>/()>>/<<<!)<(*/(!*!**)(>@>@()*)
(*/</(/*)<)(@!)(*)@/**/@//!>))<(/)!//))</@))))><(@@/(@!//!(>>>><<)>/*<>)@)**>)/@>!)/<!>!(*<**
/*)!@>(@>//!@(>)*(<>*(/)/((>*<<)@*/!*!(*(>><(!*<*!(*<@/>())/<@<</>!//!*<***@<>/@)>!/()(>!/!@>>
@!<@@<()@)<))(*/@>**(<*/*/!@**(>@*(>@)!**!*)>@))/(//!@()/!!)/*@<)!)@@/@*)@!>/)@/<!(><@
/<@*<<<)/)*<(<*(<@>*/@(>/>!)<<!()(>/>@!)<(!<*/@><<></)(<@!*!)<<!)>!/*!!/<!@)/>**)>!//)!<*/)//@!
>!@)@>*<@>!</@*@)>(<((><!!!@)@))))>)(**/@*(!*<(/(/>!/*>!*)>!)*@/>>>)(>>**((/*!(@<!*<>@)//@>(
<@/<>*()<!*)/*@@/*>))<<>*(<!@@*)!))*!>*<)*>@**/(>!!@*/@<!>/(*(>(</)*!(()>!!)!*/)/<((!>/</@!>@>
@()/)(!))@/((*@*<*(@>/(>@(/)/<*!**(</(!>!(!/*@(<!>@!@!!*@)!)/(/(*@*>@*<@*(/(*)@(!>*))<<(<>
((/(>(*!(*>(///*)(@)</)<<)*)))>))<!>(/<<)*/!/@!(/<(<///!*<*@**)>)(/<@>)/<!@()<!<!<@<*/!*(///)@/(@
//*)(!<@/<@<(@*(*@!/>!<)())<!!<*<)*((<)>@!*/!/**)!(/(*!)/!(@<>((/(>!<>@!@(*(>/!*>!!>>!!(<</<@/!>
(**)()!)(*(>()>@/(@)@/*!()*/<@<)/(*>((<@<//(@(//<!@<<*!>*(!((!*!/)()/@**/!<!@/(((*/(!</(>)(>//
>@))/(</>*(/>@/(<)*!<>*>@(*@*)*@!*)!@@>)@>**/>*!<<>/)(!)!)<@><<>!*)!(@!<(!)//<>)/(!)>><(@(@
/@)@<(><<!@(@*)<*<</()@(((@((@@>*(*!*!/((<((@/>!</@)!!>/()>>/<<<!)<(*/(!*!**)(>@>@()*))>/
/</(/*)<)(@!)(*)@/**/@//!>))<(/)!//))</@))))><(@@/(@!//!(>>>><<)>/*<>)@)**>)/@>!)/<!>!(*<**!@
/*)!@>(@>//!@(>)*(<>*(/)/((>*<<)@*/!*!(*(>><(!*<*!(*<@/>())/<@<</>!//!*<***@<>/@)>!/((>!/!@>>!
<@@<()@)<))(*/@>**(<*/*/!@**(>@*(>@)!**!*)>@))/(//!@()/!!)/*@<)!)@@/@*)@!>/)@/<!(><@
@*<<<)/)*<(<*(<@>*/@(>/>!)<<!()(>/>@!)<(!<*/@><<></)(<@!*!)<<!)>!/*!!/<!@)/>**)>!//)!<*/)//@!(<
)*<@>!</@*@)>(<((><!!!@)@))))>)(**/@*(!*<(/(/>!/*>!*)>!)*@/>>>)(>>**((/*!(@<!*<>@)//@>((/**!)@
@@/@)@<(><<!@(@*)<*<</()@(((@((@@>*(*!*!/((<((@/>!</@)!!>/()>>/<<<!)<(*/(!*!**)(>@>@()*)
(*/</(/*)<)(@!)(*)@/**/@//!>))<(/)!//))</@))))><(@@/(@!//!(>>>><<)>/*<>)@)**>)/@>!)/<!>!(*<**
/*)!@>(@>//!@(>)*(<>*(/)/((>*<<)@*/!*!(*(>><(!*<*!(*<@/>())/<@<</>!//!*<***@<>/@)>!/()(>!/!@>>
@!<@@<()@)<))(*/@>**(<*/*/!@**(>@*(>@)!**!*)>@))/(//!@()/!!)/*@<)!)@@/@*)@!>/)@/<!(><@
/<@*<<<)/)*<(<*(<@>*/@(>/>!)<<!()(>/>@!)<(!<*/@><<></)(<@!*!)<<!)>!/*!!/<!@)/>**)>!//)!<*/)//@!
!@)@>*<@>!</@*@)>(<((><!!!@)@))))>)(**/@*(!*<(/(/>!/*>!*)>!)*@/>>>)(>>**((/*!(@<!*<>@)//@>(
@@/@)@<(><<!@(@*)*<</()@(((@((@@>*(*!*!/((<((@/>!</@)!!>/()>>/<<<!)<(*/(!*!**)(>@>@()*)
(*/</(/*)<)(@!)(*)@/**/@//!>))<(/)!//))</@))))><(@@/(@!//!(>>>><<)>/*<>)@)**>)/@>!)/<!>!(*<**
/*)!@>(@>//!@(>)*(<>*(/)/((>*<<)@*/!*!(*(>><(!*<*!(*<@/>())/<@<</>!//!*<***@<>/@)>!/()(>!/!@>>
@!<@@<()@)<))(*/@>**(<*/*/!@**(>@*(>@)!**!*)>@))/(//!@()/!!)/*@<)!)@@/@*)@!>/)@/<!(><@
/<@*<<<)/)*<(<*(<@>*/@(>/>!)<<!()(>/>@!)<(!<*/@><<></)(<@!*!)<<!)>!/*!!/<!@)/>**)>!//)!<*/)//@!
>!@)@>*<@>!</@*@)>(<((><!!!@)@))))>)(**/@*(!*<(/(/>!/*>!*)>!)*@/>>>)(>>**((/*!(@<!*<>@)//@>(
<@/<>*()<!*)/*@@/*>))<<>*(<!@@*)!))*!>*<)*>@**/(>!!@*/@<!>/(*(>(</)*!(()>!!)!*/)/<((!>/</@!>@>
```

R3D
Red en Defensa
de los Derechos Digitales

Unión
Europea