Diez consideraciones para el uso y despliegue de tecnologías de reconocimiento facial

La tecnología de reconocimiento facial (TRF) es un concepto amplio que se utiliza para describir el procesamiento automático de imágenes digitales, las cuales contienen rostros de personas para la identificación, autenticación o categorización de las mismas. La identificación supone la comparación de la plantilla de una persona con una serie de plantillas en una base de datos para conocerla. La autenticación se genera tras la comparación de dos plantillas biométricas para determinar si la persona que se muestra en las dos plantillas es la misma. Por último, la categorización se utiliza para perfilar personas en función de sus características personales, como sexo, edad y origen étnico.

Para tal fin, la TRF puede implicar:

El despliegue de un monitoreo masivo y generalizado aplicable a todas las personas.

La recopilación, almacenamiento, análisis y otros tipos de tratamiento de datos personales sensibles, como lo son los datos biométricos y datos de características protegidas por el derecho a la igualdad, como la raza, el origen étnico, el género, la edad y el estado de discapacidad de las personas.

Un Estado de vigilancia masiva[1] y el tratamiento indiscriminado de datos personales anulan el derecho a permanecer en el anonimato, y tienen la capacidad de generar un efecto paralizador en la libertad de expresión y en la libertad de movimiento de las personas, alterando su comportamiento en espacios públicos y privados. En cuanto al derecho a la protesta, el uso de TRF puede ir en detrimento de una democracia participativa basada en la exigencia de derechos por fuera de canales estrictamente institucionales. El despliegue de esta tecnología puede generar un efecto inhibitorio, por el cual las personas alteren su comportamiento y se abstengan de ejercer legalmente su libertad de reunión y asociación por temor a posibles consecuencias negativas. Además, la implementación de TRF en los espacios públicos también podría usarse para perseguir a categorías específicas de individuos, como periodistas y activistas, y por lo tanto, el efecto paralizador es aún más fuerte sobre estas personas.

Por lo tanto, el uso de estas tecnologías trasciende implicaciones meramente éticas, ya que genera afectaciones directas en los derechos humanos. En la mayoría de los casos, su uso no es legítimo ni es una interferencia proporcional a los derechos a la privacidad, a la igualdad, a la libertad de expresión, a la libertad de asociación y a la libertad de reunión pacífica de las personas. Su implementación tampoco es necesaria, ya que los estudios muestran que la TRF falla en términos de precisión, con sesgos raciales sustanciales y porcentajes de resultados falsos en hasta el 80% de los casos.

La implementación de TRF, como interferencia directa e indirecta al derecho a la libertad de expresión, debe estar determinada por una vía legal, tener una finalidad legítima y ser necesaria y proporcionada para los fines que persigue. Asimismo, desde ARTICLE 19 reiteramos la necesidad de garantizar las siguientes consideraciones en aras de resguardar éste y otros derechos y libertades a la luz de la implementación de dichas tecnologías:

01.

Garantizar la implementación de marcos jurídicos robustos que regulen con claridad las facultades de vigilancia estatal (incluyendo controles estrictos en la adquisición, licitaciones, y uso de tecnologías de monitoreo, instrumentos de control judicial, auditorías, mecanismos de transparencia y otras medidas de rendición de cuentas) y la protección de datos personales. Cesar el uso de todo tipo de TRF hasta en tanto no se garantice la implementación de dichos marcos jurídicos.

02.

Prohibir el uso, implementación, importación y compra de TRF con fines de vigilancia masiva.

03.

Realizar y transparentar evaluaciones de impacto en los derechos humanos de forma regular y continua, generadas antes de la implementación de la TRF y durante todo el ciclo de uso de la misma. Lo anterior incluye evaluar los sesgos en los algoritmos utilizados en los sistemas, las amenazas planteadas por el uso de TRF para realizar vigilancia, los riesgos del tratamiento de datos personales sensibles y cualquier otra actividad que interfiera con los derechos humanos.

04.

Garantizar que las adquisiciones de un sistema de TRF o componentes de la misma por parte del Estado estén debidamente documentadas, fundadas y motivadas, y sean abiertas y transparentes. Esto incluye contratos públicos, así como asociaciones público-privadas. Lo anterior implica la publicación del propósito del uso de la TRF, metas, parámetros, licitaciones y otra información para facilitar la comprensión de la compra. Las adquisiciones deben incluir un período para comentarios del público, y los Estados deben comunicarse con los grupos potencialmente afectados cuando sea relevante para garantizar la oportunidad de realizar aportaciones.

05.

Proporcionar transparencia y rendición de cuentas en el despliegue de la tecnología con respecto a su propósito, cómo se usa, cómo funciona, quién tiene acceso a ella, quién la opera, y sus resultados con respecto a las condiciones de seguridad pública en determinado territorio, lo cual debe continuar durante todo el ciclo de uso de la TRF. Además, se deben generar informes claros y accesibles del funcionamiento y resultados de cualquier TRF.

06.

Garantizar, a través de las leyes de protección de datos personales, que las personas conozcan cómo y cuándo se recopilan sus datos biométricos, y que tengan la capacidad de no participar en implementaciones invasivas de estas tecnologías a través del consentimiento informado. La información de las locaciones donde las TRF se despliegan deben ser de conocimiento público para que la población conozca qué espacios públicos se encuentran monitoreados por el Estado.

07.

Asegurar las salvaguardas que garanticen la investigación y la reparación contra los abusos de las TRF que se presenten más allá de los objetivos para los cuales originalmente estaba planeado utilizarse. Estas previsiones deben permitir que las personas cuenten con mecanismos de protección ante posibles abusos e ilegalidades en el despliegue de las TRF.

08.

Incorporar medidas para mitigar los riesgos identificados y evitar que se produzcan violaciones de derechos, incluidas aquellas salvaguardas legales y tecnológicas que tengan que ser desarrolladas para garantizar la seguridad de los datos almacenados y para proteger los derechos humanos.

09.

Establecer responsabilidades y procedimientos de reparación ante violaciones de derechos humanos en el despliegue de dichas tecnologías y evaluar los usos de la TRF, incluyendo abordar cualquier sesgo integrado o impactos discriminatorios que pueda tener.

10.

Garantizar auditorías realizadas por personas expertas independientes a los sistemas y a los datos, sujetas a revisiones periódicas y al escrutinio de la sociedad civil y cuerpos colegiados que monitoreen el apego del despliegue de estas tecnologías a los derechos humanos.

Las recomendaciones aquí señaladas se plantean haciendo frente al clima de desconfianza de la población hacia el Estado y a las historias de vigilancia contra personas periodistas, activistas y defensoras de derechos humanos, sobre todo en los contextos de América Latina. Las experiencias de abuso, corrupción y colusión de éste con el crimen organizado hacen más imperante la necesidad de contar con controles y regulaciones que eviten el uso de las TRF para fines ilegítimos, ilegales y arbitrarios.

Fuentes consultadas:

Access Now, *Human rights in the age of artificial intelligence*, 2018, disponible en https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

Access Now, *Human Rights In The Age Of AI: A Case Study Examining Law Enforcement Use Of AI-Powered Facial Recognition*, disponible en https://www.accessnow.org/cms/assets/uploads/2018/11/ai-and-human-rights-case-study.pdf

Amnesty International, *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance*, 2020, disponible en https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/

ARTICLE 19, *UK: Government must not adopt facial recognition for immunity passports, 2020*, disponible en https://www.article19.org/resources/uk-government-must-not-adopt-facial-recognition-for-immunity-passports/

ARTICLE 19, *et. al.*, *Reclaim Your Face*, disponible en https://reclaimyourface.eu/

European Digital Rights, *Ban Biometric Mass Surveillance*, disponible en https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

Nota final:

1 Acciones para recoger, almacenar, tratar y/o analizar en secreto comunicaciones privadas y datos personales de una determinada población.