7 de junio de 2021

Carta abierta para solicitar una prohibición global sobre el uso de las tecnologías de reconocimiento facial y reconocimiento biométrico remoto que facilitan la vigilancia orientada, masiva y discriminatoria.

Quienes firmamos esta carta, queremos solicitar la prohibición total del uso de las tecnologías de reconocimiento facial y reconocimiento biométrico remoto que facilitan la vigilancia masiva, orientada y discriminatoria. Estas herramientas tienen la capacidad de identificar, seguir, encontrar y rastrar a las personas adondequiera que vayan, lo cual debilita nuestros derechos humanos y libertades civiles, incluidos los derechos a la privacidad y la protección de los datos personal, el derecho a la libertad de expresión, el derecho a la libertad de reunión y asociación (criminalizando las protestas, lo cual tiene un efecto paralizante) y los derechos a la igualdad y la no discriminación.

De hecho, hemos sido testigos de cómo las tecnologías de reconocimiento facial y reconocimiento biométrico remoto se han utilizado para violar una gran cantidad de derechos humanos. En China, Estados Unidos, Rusia, Inglaterra, Uganda, Kenia, Eslovenia, Birmania, los Emiratos Árabes Unidos, Israel y la India, la vigilancia de los ciudadanos y manifestantes ha debilitado los derechos de las personas a la privacidad y a la libertad de reunión y asociación. Los arrestos injustos de personas inocentes en los Estados Unidos, Argentina y Brasil han socavado los derechos a la privacidad, los debidos procesos y la libertad de movimiento. La vigilancia de las minorías étnicas y religiosas, así como otras comunidades marginadas y oprimidas en China, Italia y Tailandia, representa violaciones de sus derechos a la igualdad y la no discriminación.

Por diseño, estas tecnologías representan una amenaza para los derechos de las personas y ya han causado daños significativos. Ninguna salvaguarda legal o técnica podría ser suficiente para eliminar completamente el peligro que implican, y, por eso, creemos que no se deben utilizar en ningún caso en espacios públicos o de acceso público, ya sea por gobiernos o el sector privado. El potencial de abuso es demasiado grande, y las consecuencias, demasiado graves.

Solicitamos la prohibición porque, si bien una moratoria podría detener temporalmente el desarrollo y el uso de estas tecnologías, y conseguir tiempo para recopilar evidencia y organizar el debate democrático, ya es claro que estas investigaciones y discusiones solo reafirmarían que **su uso en espacios de acceso público es incompatible con los derechos humanos y las libertades civiles, y se debe prohibir completa y definitivamente.**

El alcance de nuestro pedido

Los términos "reconocimiento facial" y "reconocimiento biométrico remoto" comprenden una amplia variedad de tecnologías que incluyen desde el sistema de autenticación facial que bloquea un teléfono o autoriza el acceso a ciertos lugares, hasta la tecnología que identifica nuestra forma de caminar y los sistemas que afirman detectar la identidad de género o el estado emocional de las personas.

Nuestro pedido de una prohibición se centra, aunque no de forma excluyente, en el uso de estas tecnologías para identificar o distinguir a una persona de un conjunto más grande de individuos, lo que también se conoce como "identificación" facial o biométrica (es decir, coincidencia de uno a varios). Nos preocupa el uso de estas tecnologías para identificar, encontrar o rastrear personas mediante su rostro, su forma de caminar, su voz, su aspecto o cualquier otro identificador biométrico de un modo que permita la vigilancia masiva o la vigilancia orientada y discriminatoria, es decir, la vigilancia que tiene un impacto desproporcionado en los derechos humanos y las libertades civiles de las minorías religiosas, étnicas o raciales, las disidencias políticas y otros grupos marginados. También sabemos que, en algunos casos, los sistemas de "autenticación" biométrica o facial (coincidencia de uno a uno) se pueden implementar de un modo que permite establecer formas de vigilancia problemáticas, por ejemplo, mediante la creación de grandes bases centralizadas de datos biométricos que se puedan reutilizar con otros propósitos.

Si bien algunas aplicaciones del reconocimiento facial y el reconocimiento biométrico remoto afirman proteger la privacidad de las personas, ya que no vinculan los datos con su identidad legal, aún pueden utilizarse para encontrar personas en espacios públicos o hacer deducciones respecto de sus atributos o comportamientos. En todas estas situaciones, no importa si los datos se anonimizan para proteger la información identificable a nivel personal, o si solo se procesan localmente ("on the edge"); el daño a los derechos se produce de todas formas, porque estas herramientas están diseñadas fundamentalmente para vigilar a las personas de un modo que es incompatible con nuestros derechos.

De hecho, muchas aplicaciones de técnicas de clasificación facial y biométrica, las cuales realizan suposiciones y predicciones sobre aspectos como el género, las emociones, o bien otros atributos personales, presentan problemas fundamentales en su sustento científico. Esto significa que las inferencias acerca de las personas, con frecuencia, son no válidas debido a teorías eugenecistas de frenología y fisionomía que perpetúan la discriminación y agregan un nuevo nivel de daño a raíz de la caracterización incorrecta, además de la vigilancia.

Nuestro pedido de una prohibición comprende el uso de estas tecnologías con fines de vigilancia en espacios de acceso público y en espacios que las personas no pueden evitar. Si bien el uso lícito de estas tecnologías ha captado mucha atención y críticas, la implementación por parte de agentes privados puede suponer los mismos riesgos para nuestros derechos, en especial, cuando este sector

aplica técnicas de vigilancia en nombre de gobiernos e instituciones públicas mediante asociaciones público-privadas, o proporciona la información obtenida por estos medios a las autoridades.

También hemos notado un desarrollo preocupante en la actividad de proveedores de tecnologías de reconocimiento facial que recopilan y amalgaman bases de datos de personas "sospechosas" y las comparten con diversos clientes. Esto permite crear "bases de datos nacionales" compartidas entre empresas privadas, cuya recopilación de información queda en manos de personal no capacitado, no se sujeta a ninguna supervisión y puede generar discriminación hacia las personas que figuran en determinadas listas de vigilancia en todas las premisas en las que se usan dichas bases de datos.

El uso de estas tecnologías para vigilar a las personas en parques urbanos, escuelas, bibliotecas, lugares de trabajo, estaciones de transporte, estadios deportivos, desarrollos de viviendas y hasta en espacios en línea, como plataformas de redes sociales, representa una amenaza existencial a nuestros derechos humanos y libertades civiles, y debe detenerse.

¿Por qué pedimos una prohibición?

Las tecnologías de reconocimiento facial y reconocimiento biométrico remoto presentan una cantidad significativa de problemas técnicos en sus formatos actuales, entre ellos, los sistemas de reconocimiento facial que reflejan sesgos raciales y ofrecen menor precisión para las personas con tonos de piel más oscuros. Y aplicar mejoras técnicas a estos sistemas no eliminará los riesgos que suponen para nuestros derechos humanos y libertades civiles.

Si bien agregar datos más diversos para el aprendizaje o tomar otras medidas para mejorar la precisión pueden resolver algunos de los problemas de estos sistemas, en última instancia, estas acciones solo ayudarán a perfeccionarlos como instrumentos de vigilancia y aumentarán su efectividad para socavar nuestros derechos.

Estas tecnologías implican dos riesgos importantes para nuestros derechos:

En primer lugar, los datos de aprendizaje (las bases de datos de rostros con las que se comparan las entradas de datos, y los datos biométricos que procesan estos sistemas), con frecuencia, se obtienen sin el conocimiento, el consentimiento o la libre elección de las personas para la recopilación, lo que significa que estas tecnologías promueven la vigilancia masiva y la vigilancia orientada y discriminatoria por diseño.

En segundo lugar, mientras las personas se puedan identificar, encontrar o rastrear inmediatamente en espacios de acceso público, sus derechos humanos y libertades civiles se verán perjudicados. Incluso la idea de que las tecnologías de este tipo pueden implementarse en espacios de acceso público tiene un efecto paralizante, lo cual debilita la capacidad de las personas de hacer uso de sus derechos.

7 de junio de 2021

A pesar de las afirmaciones cuestionables sobre la mejora de la seguridad pública que prometen estas tecnologías, los beneficios no compensan las violaciones sistemáticas de nuestros derechos. A su vez, el abuso y la implementación de estas tecnologías con niveles de transparencia bajos o nulos es cada vez más evidente.

Cualquier sondeo o análisis sobre la implementación histórica de metodos de vigilancia demuestra que el uso experimental de estas tecnologías con frecuencia criminaliza a las comunidades marginadas y de bajos ingresos, incluidas las de color, es decir, las mismas comunidades que tradicionalmente han sufrido de discriminación y racismo estructurales. El uso de tecnologías de reconocimiento facial y reconocimiento biométrico remoto no es la excepción a esto, y, por lo tanto, debe erradicarse antes de que se cree o se implemente permanentemente una estructura de vigilancia aún más peligrosa.

La mera existencia de estas herramientas, ya sea que se encuentren en manos de las autoridades públicas o empresas privadas (o asociaciones público-privadas), siempre implicará un incentivo para los usos con fines diferentes de los planificados y el aumento de la vigilancia en espacios públicos, lo cual tiene un efecto paralizante en la libertad de expresión. Dado que su existencia pone en peligro nuestros derechos y que no es posible implementar una supervisión efectiva que impida los abusos, no queda opción más que prohibir completamente su uso en los espacios de acceso público.

¿Qué tipo de prohibición pedimos?

Algunas tecnologías de vigilancia son simplemente tan peligrosas que generan muchos más problemas que los que resuelven. Cuando se trata de tecnologías de reconocimiento facial y reconocimiento biométrico remoto que posibilitan la vigilancia masiva, discriminatoria y orientada, el potencial de abuso es demasiado significativo, y las consecuencias, demasiado graves.

No hay margen para la duda: a fin de proteger los derechos humanos y las libertades civiles, se debe prohibir completamente el uso de estas tecnologías en espacios de acceso público a nivel nacional, estatal, provincial, local, incluidas todas sus subdivisiones y autoridades, y, en especial, a nivel de las autoridades de implementación y control fronterizo, que ya tienen suficientes recursos humanos y tecnológicos para mantener la seguridad sin necesidad de utilizar herramientas de este tipo.

Como red global de organizaciones de sociedad civil, reconocemos que cada país tiene una manera distinta de desarrollar soluciones que prioricen los derechos humanos en sus sistemas legales, convencionales o constitucionales.

Sin embargo, independientemente de los medios, el resultado debe ser la prohibición total del uso de estas tecnologías para vigilar, identificar, encontrar, clasificar y rastrear personas en espacios de acceso público.

Por todos estos motivos, este es nuestro pedido:

1.) **A las personas a cargo de formular políticas públicas y leyes en todos los niveles de gobierno** y en todo el mundo, les pedimos lo siguiente:
   a. Detener todas las inversiones públicas en el uso de tecnologías de reconocimiento facial y reconocimiento biométrico remoto que permitan la vigilancia masiva y la vigilancia discriminatoria y orientada
   b. Adoptar leyes, estatutos y normativas integrales que:
      i. Prohiban el uso de estas tecnologías para la vigilancia de los espacios públicos y de acceso público, incluidos los medios de transporte públicos, ya sea en nombre de los gobiernos nacionales, federales, estatales, provinciales, municipales, locales u otras subdivisiones políticas, incluidas sus agencias, departamentos, secretariados, ministerios, oficinas ejecutivas, consejos, comisiones, departamentos, o sus contratistas o demás subdivisiones y autoridades, con especial énfasis en las agencias de implementación, investigación criminal, control fronterizo y de inteligencia
      ii. Prohiban el uso de estas tecnologías por parte de entidades privadas en espacios públicos, de acceso público y lugares de alojamiento público, donde dicha implementación podría facilitar la vigilancia masiva y la vigilancia orientada y discriminatoria, incluidos, entre otros, su uso en parques, escuelas, bibliotecas, lugares de trabajo, estaciones de transporte, estadios deportivos y desarrollos habitacionales
      iii. Prohiban a las agencias gubernamentales, en especial las de implementación, el uso y acceso a los datos y la información que deriven del uso de dichas tecnologías por parte de empresas privadas y otros agentes privados, salvo para fines de auditorías o comprobaciones de cumplimiento
      iv. Protejan a las personas del uso de estas tecnologías para tomar decisiones en asuntos relacionados con los derechos económicos, sociales y culturales, incluidos la vivienda, el empleo, los beneficios sociales y la atención médica
      v. Excluyan el uso de estas tecnologías y la información obtenida a partir de ellas, como evidencia para procesar o acusar a personas a fin de encarcelarlas o detenerlas de cualquier modo
      vi. Restrinjan el acceso gubernamental a la información biométrica almacenada por las empresas privadas
   c. Establecer reglas y normativas que prohíban la adquisición de estas tecnologías por parte de gobiernos y agencias estatales con fines de uso que faciliten la vigilancia masiva y la vigilancia discriminatoria y orientada
   d. Dejar de utilizar las tecnologías de reconocimiento facial y reconocimiento biométrico remoto para la vigilancia masiva y la vigilancia discriminatoria y orientada de minorías

religiosas, étnicas y raciales, así como las disidencias políticas y otros grupos marginados

e. Ordenar la divulgación del uso de este tipo de tecnologías ante quienes se hayan sometido a ellas sin conocimiento y no hayan tenido la posibilidad de ejercer sus derechos de debido proceso para impugnar su uso
f. Proporcionar indemnizaciones adecuadas a quienes se vean perjudicados por el uso de estas tecnologías

---

2.) **A las cortes y quienes desempeñan funciones judiciales**, les pedimos que reconozcan las amenazas existenciales a los derechos humanos que implica el uso de estas tecnologías y que tomen medidas para prevenirlas, y, si es necesario, que rectifiquen los daños derivados de su uso.

3.) **A las agencias administrativas**, incluidas las de protección de datos personales y de protección del consumidor, les solicitamos que utilicen todo el alcance de su autoridad para proteger la privacidad y los derechos de los consumidores y las consumidoras, incluso cuando esto implique instar a las empresas a suspender el uso de dichas tecnologías.

Por último, reconocemos que las amenazas existenciales que conllevan las tecnologías de reconocimiento facial y reconocimiento biométrico remoto no solo se deben abordar a nivel de cada país y cada gobierno, sino que también deben intervenir otros actores importantes de los niveles nacional e internacional.

Por este motivo, hacemos los siguientes pedidos:

1.) **A las organizaciones internacionales, como la Oficina del Alto Comisionado para los Derechos Humanos de la ONU (OHCHR),** les pedimos que condenen el desarrollo y el uso actuales de las tecnologías de reconocimiento facial y reconocimiento biométrico remoto para vigilar a las comunidades en todo el mundo

---

2.) A las **entidades privadas** que desarrollan o utilizan tecnologías de reconocimiento facial o reconocimiento biométrico remoto, les solicitamos lo siguiente:

a. Comprometerse públicamente a cesar la creación, el desarrollo, la venta y el uso de tecnologías de reconocimiento facial y reconocimiento biométrico remoto que facilitan la vigilancia masiva y la vigilancia discriminatoria y orientada
b. Detener inmediatamente la producción de tecnologías de reconocimiento facial y reconocimiento biométrico remoto que facilitan la vigilancia masiva y la vigilancia discriminatoria y orientada, y que eliminen cualquier dato biométrico obtenido de

forma no legítima y utilizado para crear bases de datos y modelos o productos basados en ellos

c. Elaborar informes de transparencia con detalles sobre todos sus contratos públicos (incluidos los que se encuentran suspendidos, en curso o en proceso) para la provisión de estas tecnologías
d. Apoyar a la comunidad trabajadora (y abstenerse de tomar represalias contra ellos) que organice en sus lugares de trabajo maneras de desafiar o rechazar el desarrollo de las tecnologías de reconocimiento facial y reconocimiento biométrico remoto que faciliten la vigilancia masiva y la vigilancia discriminatoria y orientada

---

3.) **A quienes trabajan en empresas de tecnología**, les pedimos que, con el respaldo de sus sindicatos, se organicen en sus lugares de trabajo para rechazar el desarrollo o la venta de las tecnologías de reconocimiento facial y reconocimiento biométrico remoto en la mayor medida posible

---

4.) **A la comunidad de inversionistas y las instituciones financieras**, les pedimos lo siguiente:

a. Llevar a cabo debidas diligencias de cumplimiento de derechos humanos con respecto a sus inversiones actuales y futuras en las empresas que desarrollan y venden tecnologías de reconocimiento facial y reconocimiento biométrico remoto a fin de detectar instancias en las que estas tecnologías sean incompatibles con los derechos humanos y facilitan la vigilancia masiva y la vigilancia discriminatoria y orientada
b. Solicitar a las empresas que reciben sus inversiones que detengan la creación, el desarrollo, la venta y cualquier prestación relacionada con la provisión de estas tecnologías de modos que faciliten la vigilancia masiva y la vigilancia discriminatoria y orientada

---

5.) A las **organizaciones donantes**, les pedimos que dispongan de fondos para los litigios estratégicos y las campañas de incidencia de las organizaciones no gubernamentales y de la sociedad civil que se dedican a obtener reparaciones por daños en los tribunales de justicia y que participan activamente en la formulación de políticas públicas a nivel local, estatal, provincial, nacional, federal, supranacional, regional e internacional.

Conclusión

Instamos a la sociedad civil, las agrupaciones de activistas, las comunidades académicas y otras partes interesadas de todo el mundo a firmar esta carta y unirse en la lucha para garantizar que el uso de estas tecnologías en espacios de acceso público se prohíba ahora y de forma definitiva para proteger los derechos humanos y las libertades civiles.

Comuníquese con **banBS@accessnow.org** para obtener más información sobre cómo puede apoyar esta iniciativa y visite **accessnow.org/ban-biometric-surveillance** para ver la lista completa de signatarios y agregar su nombre a la lista.

Esta declaración fue redactada por Access Now, Amnistía Internacional, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF) y el Instituto Brasileiro de Defesa do Consumidor (IDEC)