

Ciudad Autónoma de Buenos Aires, 22 de septiembre de 2021

JUZGADO DE 1RA INSTANCIA EN LO CONTENCIOSO ADMINISTRATIVO Y TRIBUTARIO N°  
2

HONORABLE MAGISTRADO  
ROBERTO ANDRÉS GALLARDO

---

**SE PRESENTAN EN CALIDAD DE AMICUS CURIAE**

---

**Sr juez:**

Maria Soledad Marinaro, abogada, inscripta al TOMO 119 FOLIO 726 del C.P.A.C.F constituyendo domicilio procesal en Av General Hornos 1024 de la Ciudad Autónoma de Buenos Aires y domicilio electrónico en 27230044231, en mi carácter de letrada apoderada de Peter Micek, representante legal de la organización internacional de derechos humanos Access Now, en la causa “OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO **O.D.I.A. CONTRA GCBA SOBRE AMPARO - OTROS**”, EXPTE N° 182908/2020-0, **que tramita ante vuestro tribunal, me presento y respetuosamente digo:**

**ACREDITA PERSONERÍA-HACE SABER**

I- Que vengo acreditar personería mediante copia simple de poder especial otorgado por el Sr Peter Micek, ciudadano de los Estados Unidos de América, de profesión abogado, nacido el 15 de junio de 1981 con domicilio en Brooklyn, New York.

Declaro bajo juramento que el poder mencionado se encuentra plenamente vigente y sin limitaciones de naturaleza alguna.

II- Se hace saber que a la fecha se encuentra en trámite las legalizaciones con respecto a las gestiones del apostillado conforme convenio de la Haya del 5/10/1961, y también se encuentra pendiente la traducción pública pertinente.

**I. OBJETO**

1. Venimos a presentar este documento de amicus curiae a los fines de exponer nuestra opinión experta en materia del impacto de las tecnologías de vigilancia cuestionadas en esta causa en los derechos humanos, especialmente en relación a la privacidad, la libertad de reunión, la libertad de expresión y el derecho a la no discriminación.

**II. LEGITIMACIÓN**

2. Access Now es una organización global de la sociedad civil dedicada a defender y extender los derechos digitales de los usuarios y las usuarias en riesgo<sup>1</sup>. A través de su representación en diez países de todo el mundo, Access Now proporciona liderazgo a través de campañas de incidencia y recomendaciones de políticas públicas a los sectores público y privado para garantizar el acceso y correcto funcionamiento de Internet y la protección de los derechos fundamentales para lo cual cuenta con una comunidad global centrada en la acción de casi medio millón de usuarios y usuarias de más de 185 países. Access Now también cuenta una línea de ayuda de seguridad digital las 24 horas del día, los 7 días de la semana, que brinda asistencia técnica directa en tiempo real a las comunidades afectadas y personas vulnerables de todo el mundo. Access Now es no partidista, sin fines de lucro y no está afiliado a ningún país, corporación o religión.
3. Access Now ha presentado escritos de amicus curiae sobre cuestiones relacionadas con los derechos digitales en jurisdicciones nacionales en numerosas oportunidades, incluidos los Estados Unidos, Camerún e Indonesia<sup>2</sup>. Access Now también lo ha hecho ante tribunales regionales, como el Tribunal Europeo de Derechos Humanos y el Tribunal de Justicia de la Comunidad Económica de los Estados de África Occidental (CEDEAO)<sup>3</sup>. Los temas de estas presentaciones incluyen cierres de Internet, bloqueo de sitios web, responsabilidad de las plataformas en línea por contenido generado por terceros, privacidad de los datos y vigilancia. En 2016, Access Now recibió estatus consultivo especial ante el Consejo Económico y Social (ECOSOC) de las Naciones Unidas (ONU). Access Now también ha publicado una serie de publicaciones que tratan temas de privacidad, inteligencia artificial, protección de datos personales y uso del reconocimiento facial<sup>4</sup>.
4. Amicus Curiae. En nuestra realidad jurídica se encuentra incorporado y con gran aceptación la figura del amicus curiae, vinculada con antecedentes en el derecho internacional de derechos humanos, siendo reconocida por nuestros tribunales nacionales e internacionales. A nivel nacional encuentra su base en el art 33 de la CN. La Corte Suprema de Justicia no solo toma como fundamento nuestra CN sino que reconoce ,conforme el art 36 del CPCCN, la escucha de opiniones de entidades o

1 Más información disponible en: <https://www.accessnow.org/about-us/>

2 Mas información disponible en: <https://www.accessnow.org/access-now-joins-legal-brief-supporting-privacy-facebook-users/> , <https://www.accessnow.org/access-now-isf-file-legal-intervention-cameroon-shutdown/>, y <https://www.accessnow.org/indonesians-seek-justice-after-internet-shutdown/>.

3 Mas información disponible en: <https://www.accessnow.org/website-blocking-russia-goes-european-court-human-rights-access-now-intervenes/>, <https://www.accessnow.org/delfi-as-v-estonia-a-blow-to-free-expression-online/>, <https://www.statewatch.org/news/2018/dec/echr-hu-magyar-jeti-zrt-v-hungary-hyperlinks-defamation-judgement-4-12-18.pdf>, <https://www.accessnow.org/cms/assets/uploads/2016/02/ECTHRIIntervention.pdf>, and <https://www.accessnow.org/judges-raise-the-gavel-to-keepit-on-around-the-world/>.

4 Mas información disponible en:

<https://www.accessnow.org/proteccion-de-datos-es-importante/>, <https://www.accessnow.org/cms/assets/uploads/2018/04/manual-de-proteccion-de-datos.pdf>, <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.

personas que no son parte del proceso a los fines de aportar una opinión vinculante y legitimada al caso.

5. La regulación de la Corte suprema a través del dictado de la acordada 28/2004, en la cual admite la posibilidad de presentar amicus curiae ante la CSJN, da cuenta de que no debería haber rechazos en instancias inferiores. En los considerandos de dicha acordada se indica: *“en el marco de las controversias cuya resolución por esta Corte genere un interés que trascienda al de las partes y se proyecte sobre la comunidad o ciertos sectores o grupos de ella, a fin de resguardar el más amplio debate como garantía esencial del sistema republicano democrático, debe imperar un principio hermenéutico amplio y de apertura frente a instituciones, figuras o metodologías que, por su naturaleza, responden al objetivo de afianzar la justicia entronizado por el Preámbulo de la Constitución”*
6. Luego a través de la acordada 7/2013 con respecto a amicus curiae manifiesta: “pluralizar y enriquecer el debate constitucional, así como de fortalecer la legitimación de las decisiones jurisdiccionales dictadas por esta Corte Suprema en cuestiones de trascendencia institucional”. Ésta acordada que regula sobre la presentación de Amigos del Tribunal tiene establecido que pueden presentarse personas -físicas o jurídicas- en calidad de Amigos del Tribunal en “todos los procesos judiciales correspondientes a la competencia originaria o apelada en los que se debatan cuestiones de trascendencia colectiva o interés general”.
7. Conforme a lo expuesto a los fines de que mi opinión pueda resultar útil en ésta causa al momento de dictar sentencia, es que vengo a presentarme en calidad de AMICUS CURIAE

### **III. RESUMEN DEL CASO Y EJE DE LA INTERVENCIÓN**

8. La presente causa identificada con el EXPTE N° 182908/2020-0 es una Acción de Amparo Colectivo presentada por el OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.) contra el GOBIERNO DE LA CIUDAD DE BUENOS AIRES, por el uso de sistemas de vigilancia masiva
9. La parte demandante sostiene que los actos administrativos y modificaciones regulatorias que hacen al Sistema de Reconocimiento Facial de Prófugos, el Sistema Preventivo y el Sistema Forense, las bases de datos y la infraestructura para su funcionamiento, son violatorios de derechos humanos consagrados por la Constitución Nacional y por los Tratados Internacionales de los cuales el País es firmante.
10. Asimismo, solicita medida cautelar de no innovar a fin de evitar los graves perjuicios que la aplicación inmediata de estos artículos y por consiguiente, de estas tecnologías, provocan.
11. Esta intervención proporcionará aclaraciones sobre varios aspectos del caso, centrándose en particular en la naturaleza de las actividades de procesamiento de datos realizadas, resaltando preocupaciones adicionales planteadas por el estado científico contencioso del “reconocimiento facial” y su impacto discriminatorio. Para ello, analizaremos: i) consideraciones preliminares: sistemas de reconocimiento facial; ii) requisitos previos a la implementación de tecnologías de vigilancia; iii) deficiencias y preocupaciones relacionadas al sistema de reconocimiento facial; iv) impacto en los

derechos humanos de los sistemas de reconocimiento facial; v) prohibición de los sistemas de reconocimiento facial; vi) posición de organismos internacionales; y vii) campañas de sociedad civil.

#### IV. CONSIDERACIONES PRELIMINARES: SISTEMAS DE RECONOCIMIENTO FACIAL

12. A los fines de esclarecer los procesos involucrados en la tecnología de reconocimiento facial y entender su impacto en los derechos humanos, utilizaremos una serie de definiciones sobre tecnologías biométricas esbozadas por el **Grupo de Trabajo de Protección de Datos del Artículo 29 de la Unión Europea, Opinión WP193 3/2012** sobre desarrollos en tecnologías biométricas (en adelante, Opinión del Grupo de Trabajo)<sup>5</sup>.
13. Según la Opinión del Grupo de Trabajo, la **fuentes de datos biométricos** puede variar considerablemente e incluye elementos físicos, fisiológicos, de comportamiento o psicológicos de un individuo. Define a los datos biométricos como “propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad”.
14. Según el art. 2 del Anexo de la Resolución 398/1, el sistema utilizado por el Gobierno de la Ciudad contrasta los datos obtenidos por las cámaras con la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC), la cual presenta serios problemas. La CONARC fue objetada por el relator especial de la ONU sobre el derecho a la privacidad, Joseph Cannataci. En su declaración el Relator observó que la base contenía datos de 61 menores de edad y “múltiples errores”, como el caso de 2 personas que figuraban “como de 2 y 3 años de edad, buscadas por asalto y robo”<sup>6</sup>. Por su parte, Marcelo D’Alessandro, secretario de Seguridad del Ministerio de Seguridad y Justicia de Buenos Aires, al ser consultado si el Gobierno previamente testeó la calidad de la base de datos y si estaba al tanto de las inconsistencias que tenía, respondió: “usamos esa base de datos porque es la única que hay sobre prófugos. Es verdad que la base de datos está desactualizada y tiene errores. Nosotros lo manifestamos. Lo que está mal es la carga de datos. Entonces, el SRFP sólo potenció un problema que ya estaba, y ahora de hecho está sirviendo para depurar la Conarc”<sup>7</sup>.
15. Una de las **técnicas biométricas** utilizadas por estos sistemas se basan en aspectos físicos y fisiológicos que miden las características fisiológicas de una persona e incluyen: comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, **reconocimiento facial**, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de muestras del ADN y análisis de los poros de la piel, etc.

5 [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193\\_es.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_es.pdf)

6 <https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=S>

7 <https://www.chequeado.com/investigacion/video-vigilancia-en-buenos-aires-la-otra-cara-del-control/>

16. Los **sistemas biométricos** son aplicaciones de las tecnologías biométricas que permiten la identificación automática, y/o la autenticación/comprobación de una persona. La Opinión del Grupo de Trabajo incluye que “debido a la evolución tecnológica reciente ahora es posible utilizar los sistemas biométricos para fines de categorización o segregación” y que “los riesgos que presentan los sistemas biométricos se derivan de la propia naturaleza de los datos biométricos utilizados en el tratamiento”.
17. La Opinión del Grupo de Trabajo identifica tres etapas típicas involucradas en el procesamiento de datos biométricos en un sistema biométrico: *registro biométrico*, *almacenamiento biométrico* y *correspondencia biométrica*. El **registro biométrico** “abarca todos los procesos que se llevan a cabo en un sistema biométrico con el fin de extraer datos biométricos de una fuente biométrica y vincular estos datos a un individuo”. La Opinión agrega que, si bien tal inscripción puede implicar pedirle a la persona su consentimiento para recopilar su información biométrica, “también es posible inscribir a personas sin su conocimiento o consentimiento (por ejemplo, sistemas de CCTV con funcionalidad de reconocimiento facial incorporada)”. Dado que el sistema de reconocimiento facial (en adelante SRF) utilizado en la Ciudad Autónoma de Buenos Aires (CABA) captura y procesa imágenes de los rostros de los transeúntes, el sistema captura y procesa datos biométricos relacionados con las características fisiológicas de los individuos sin su consentimiento.
18. Dada que la información recolectada es información sensible (lo cual será explicado con mayor detalle en la Sección VII) garantizar su seguridad es fundamental. Desafortunadamente y tal como lo expresa la parte demandante, al momento de requerir información a las autoridades, estas se negaron a brindar información específica sobre las medidas de seguridad adoptadas para proteger la información recolectada, qué tipo de información se registra, cómo se conserva, cuál es la técnica de borrado, con quiénes se comparte dicha información y con qué fines.
19. En cuanto al **almacenamiento de datos biométricos**, el Grupo de Trabajo observa que existen dos posibilidades de almacenamiento. En primer lugar, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica.
20. Una consideración importante aquí es cuánta información se almacena en una plantilla biométrica. El Grupo de Trabajo observa que existe una compensación entre la cantidad de información que contiene la plantilla y, por lo tanto, lo útil que es para su posterior procesamiento y análisis, y qué tan segura es la plantilla frente a los esfuerzos por reconstruir los datos sin procesar. El peligro aquí es que cuanto más útil y rica en información es una plantilla, mayor es el riesgo de que alguien pueda reconstruir los datos sin procesar originales, por lo general, confidenciales.
21. La definición del tamaño (la cantidad de información) de la plantilla es un tema crucial. Por un lado, el tamaño de la plantilla debe ser lo suficientemente amplio para gestionar la seguridad (evitando superposiciones entre diferentes datos biométricos o sustituciones de identidad), por otro lado, el tamaño de la plantilla no debe ser demasiado grande para evitar los riesgos de la reconstrucción de datos biométricos.

22. La etapa final en el procesamiento de datos biométricos es la **correspondencia biométrica**, que la Opinión del Grupo de Trabajo define como “el proceso de comparación de los datos o plantillas biométricas (capturados durante el registro) con los datos o plantillas biométricas recogidos en una nueva muestra a efectos de identificación, verificación y autenticación o categorización”.
23. El sistema de reconocimiento facial utilizado en la Ciudad Autónoma de Buenos Aires realiza un proceso de **identificación**. De acuerdo a la Opinión del Grupo de Trabajo, la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno -a-varios)

## V. REQUISITOS PREVIOS A LA IMPLEMENTACIÓN DE TECNOLOGÍAS DE VIGILANCIA

24. Es usual que nuestras instituciones públicas busquen solucionar complejos problemas sociales a través de la adopción de nuevas tecnologías. Sin embargo, estas herramientas no son inocuas y adoptadas de forma irreflexiva pueden conllevar un potencial daño que, lejos de cumplir el objetivo para el cual fueron implementadas, crean nuevos problemas sociales. Este uso negligente de las tecnologías es conocido como “tecnosolucionismo” y se contrapone a la idea de tecnologías adoptadas en base a evidencia, sustento científico, debate público y con suficientes medidas de seguridad que garanticen la reducción de potenciales usos abusivos y daños.
25. Para evitar la adopción irresponsable de tecnologías es fundamental aplicar los **principios de transparencia y rendición de cuentas** en su adquisición e implementación. Estos principios se encuentran garantizados en la Constitución Nacional, Artículo 1,33,41,42 y concordantes del Capítulo Segundo y del Artículo 7 inciso 22 que incorpora con jerarquía constitucional diversos tratados internacionales, a saber: Convención de las Naciones Unidas contra la Corrupción y la Convención Interamericana contra la Corrupción (propician la transparencia, el acceso a la información pública y la participación de la sociedad civil en el combate contra la corrupción (Artículos 10 y 13; párrafo 5 de su Preámbulo y artículos III.11 y XIV.2, respectivamente)); Declaración Universal de Derechos Humanos (protege el derecho de acceso a la información al establecer: “toda persona tiene derecho a la libertad de opinión y de expresión”, entendiendo que “este derecho incluye el de no ser molestado a causa de sus opiniones y el de investigar y recibir informaciones y opiniones, y el de difundirlas sin limitaciones de fronteras, por cualquier medio de expresión” (Artículo 19)); y El Pacto Internacional de Derechos Civiles y Políticos (apunta a proteger el acceso a la información y el derecho a la libertad de expresión como derecho colectivo (Artículo 19))<sup>8</sup>. Existen además normas nacionales específicas dirigidas a apuntalar este derecho, a saber: Ley 27275 de Derecho de Acceso a la Información Pública (establece la obligatoriedad para los tres poderes del Estado y entes u organizaciones con aporte estatal, de responder a la solicitud de información por parte de cualquier ciudadano en un plazo máximo de 30 días)<sup>9</sup>. La Ciudad Autónoma de Buenos Aires también

<sup>8</sup> <https://www.argentina.gob.ar/transparencia/informacion>

<sup>9</sup> *ibid*.

garantiza este derecho a través de la Ley 104 de Solicitud de información pública<sup>10</sup>, la cual tiene por objeto garantizar el derecho de toda persona a solicitar y recibir información pública de manera completa, veraz, adecuada y oportuna, sin necesidad de indicar los motivos de la solicitud.

26. En el caso de la implementación del Sistema de Reconocimiento Facial adquirido e implementado en la Ciudad Autónoma de Buenos Aires estos principios no han sido aplicados y el acceso a la información pública no ha sido garantizado. Numerosas organizaciones de la sociedad civil haciendo uso del derecho de acceso a la información pública presentaron solicitudes que fueron atendidas de forma incompleta y defectuosa. A los fines de la brevedad de la presente intervención remitimos a lo expresado por la parte demandante quien habiendo hecho uso de este derecho recibió respuestas parciales por parte del Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires que no satisficieron el pedido de información e incluso preguntas sin respuesta alguna.
27. De igual forma, la organización Asociación por los Derechos Civiles (ADC) con fecha 04 de abril de 2019 presentó Solicitud de acceso a la información pública<sup>11</sup>. En su devolución, el Ministerio de Justicia y Seguridad no respondió a la totalidad de los interrogantes<sup>12</sup>. Destacamos la falta de precisión respecto de la finalidad del sistema puesto que el Ministerio se limitó en responder que el sistema será utilizado “únicamente para tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial de la Nación, Provincial y de la Ciudad Autónoma de Buenos Aires, como así también para detección de personas buscadas exclusivamente por orden judicial, registradas en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC)”. La idea de “tareas requeridas” permite una interpretación abierta y puede dar lugar a usos abusivos del sistema. Asimismo, al ser consultado por protocolos y políticas estrictas para evitar el uso abusivo del sistema y medidas que transparente la manera en que la tecnología es utilizada, el Ministerio solo afirmó que será aplicado “el régimen disciplinario ordinario previsto en la Ley N° 5688 y su reglamentación (Decreto N° 53/17) y en la Ley N° 471 de Relaciones Laborales en el ámbito del GCBA y sus normas reglamentarias”.
28. La adquisición directa del sistema de reconocimiento facial son muestras de la falta de transparencia. En ninguna de las solicitudes de acceso a la información pública el Ministerio dió razones que justifiquen el uso de este mecanismo y no una licitación pública.
29. Esto es especialmente preocupante ya que la empresa desarrolladora del software de reconocimiento facial que utiliza DANAIDE es NTechLab. En la versión rusa del sitio web de NTechLab<sup>13</sup>, el software UltraIP<sup>14</sup> de Danaide, que se vende en Argentina, figura en la sección de socios. Como respuesta al pedido de acceso a la información de ADC de junio del 2019<sup>15</sup>, autoridades de Buenos Aires confirmaron que UltraIP es el nombre del software que licenciaba. En octubre del 2020, la organización de derechos

10 <https://www.buenosaires.gob.ar/tramites/ley-104-solicitud-de-informacion-publica>

11 <https://adc.org.ar/wp-content/uploads/2019/12/PAIP-reconocimiento-facial-MinSeg-CABA.pdf>

12 <https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/>

13 <https://web.archive.org/web/20200511205745/https://findface.pro/partners>

14 <https://danaide.com.ar/desarrollos/desarrollossoftware.html>

15 <https://adc.org.ar/wp-content/uploads/2019/07/Respuesta-PAIP-reconocimiento-facial-GCBA-V2.pdf>

humanos, Human Rights Watch, alertó al público acerca de fallas en el sistema de NTechLab y su uso indebido por parte del gobierno para identificar y usar de blanco a niños(as) por persecución penal en violación de derechos humanos<sup>16</sup>. En Moscú, NTechLab provee el software para un programa de vigilancia del que el gobierno ha abusado, según grupos de derechos humanos, mediante la vigilancia de personas durante la pandemia de COVID-19 para hacer cumplir un confinamiento<sup>17</sup>. Por principio general, los gobiernos deberían abstenerse de adquirir productos de aquellas empresas que no asuman un compromiso irrestricto con los derechos humanos.

30. Al momento de implementar tecnologías, especialmente cuando pueden implicar sistemas de vigilancia ubicuos, es esencial disponer una **etapa consultiva previa a su adquisición e implementación con los distintos sectores sociales interesados** (sociedad civil, academia, comunidad técnica, etc.). Esta instancia permite comprender los beneficios y los potenciales riesgos de las tecnologías, analizar la necesidad y proporcionalidad de la solución, permitiendo a los tomadores de decisión adoptar soluciones de forma informada.
31. En abril de 2019, el Gobierno de la Ciudad Autónoma de Buenos Aires anunció la inminente instalación de un sistema de reconocimiento facial en el espacio público de la Capital<sup>18</sup>. En ningún momento el gobierno convocó a los sectores interesados a discutir dicha tecnología e incluso reconoce que la misma fue probada sin conocimiento del público en general<sup>19</sup>.
32. Otro ejemplo de la falta de debate público fue la aprobación de la ley 1686-D-2020 que modifica a la Ley 5688 del Sistema Integral de Seguridad Pública<sup>20</sup> que incorporó el Sistema de Reconocimiento Facial de Prófugos a la normativa. Pese a las advertencias emitidas por las organizaciones que nos acercamos a los y las legisladoras y a las reuniones de comisión, el debate no se amplió ni se llevó a Comisión de Derechos Humanos y Garantías, tal como habíamos solicitado junto a varios legisladores que hicieron suya nuestra demanda de profundizar un debate necesario antes de legitimar una práctica que amenaza derechos ciudadanos<sup>21,22</sup>.
33. Otro requisito previo a la implementación de tecnologías es la **evaluación de impacto en la privacidad y en los datos personales**. Las modernas leyes en materia de protección de datos personales establecen esta evaluación de forma previa y obligatoria a los fines de determinar las bases y justificación de la necesidad y proporcionalidad en que se realizará cualquier actividad que implique el procesamiento de datos personales.
34. En esta línea, la Agencia de Acceso a la Información Pública de Argentina (AAIP) publicó la *Guía de Evaluación de Impacto en la Protección Datos*<sup>23</sup>. La AAIP reconoce en dicha guía que “la interceptación de telecomunicaciones, el monitoreo

16 <https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online>

17 <https://uk.reuters.com/article/uk-health-coronavirus-russia-facial-reco-idUKKCN2253CG>

18 <https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos>

19 *ibid.*

20 <https://parlamentaria.legislatura.gov.ar/pages/expediente.aspx?id=117084&iframe=true&width=99%&height=100%>

21 <https://adc.org.ar/wp-content/uploads/2020/09/ADC-reconocimiento-facial.pdf>

22 <https://www.vialibre.org.ar/la-legislatura-de-caba-aprobo-la-regulacion-del-reconocimiento-facial/>

23 [https://www.argentina.gob.ar/sites/default/files/guia\\_final.pdf](https://www.argentina.gob.ar/sites/default/files/guia_final.pdf)



desproporcionado de los espacios públicos a través de sistemas de videovigilancia, la recolección o publicación de datos personales sin el consentimiento de sus titulares, así como el tratamiento automatizado de información a través de algoritmos o inteligencia artificial representan algunos de los problemas que [el derecho a la protección de datos personales] intenta resolver y de los que se ocupa activamente esta rama del derecho”. Agrega a continuación que “observando con preocupación estos fenómenos de las décadas recientes y con el fin de mitigar los riesgos que entrañan, las Autoridades de Control de la República Oriental del Uruguay y de la República Argentina han decidido cooperar para diseñar un mecanismo de carácter preventivo que busca minimizar los potenciales daños a la privacidad: la Evaluación de Impacto en la Protección de Datos (EIPD).” y que “el objetivo de esta herramienta [haciendo referencia a la guía] es que, desde una etapa temprana, las prácticas y proyectos que puedan afectar los derechos de las personas, a través del tratamiento de sus datos personales, sean evaluados por los responsables de tratamiento y constituidos conforme a ciertos estándares restrictivos de seguridad y de integridad”.

35. En las respuestas obtenidas a las solicitudes de acceso a la información pública citadas en esta intervención y a la presentada por la parte demandante, el Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires reconoce no haber llevado a cabo evaluación de impacto alguna.
36. En declaración del día 17 de mayo de 2019, el Relator Especial sobre el derecho a la privacidad de las Naciones Unidas, Joseph Cannataci, luego de su visita a la Argentina, explica haciendo referencia al sistema de cámaras de vigilancia de la Ciudad que “la justificación de tal sistema, su legitimidad, necesidad y proporcionalidad deberían haberse establecido mediante una evaluación del impacto en la privacidad (en inglés Privacy Impact Assessment, PIA) que no parece haberse llevado a cabo” para luego agregar que “el hecho de que el reconocimiento facial se esté implementando sin el PIA necesario, así como la consulta deseable y las fuertes salvaguardias, también es motivo de preocupación”<sup>24</sup>.

## **VI. DEFICIENCIAS Y PREOCUPACIONES RELACIONADAS AL SISTEMA DE RECONOCIMIENTO FACIAL**

37. Los softwares de reconocimiento facial pueden llegar a tener altos porcentajes de falsos positivos. Solo para citar algunos ejemplos, las pruebas realizadas por la Metropolitan Police de Londres resultaron en un 86% de personas mal identificadas como presuntas criminales<sup>25</sup>. La Policía de Gales del Sur también ha hecho pruebas con sistemas de reconocimiento facial y ha obtenido falsos positivos en más de un 90 % de los casos<sup>26</sup>.
38. Adicionalmente los SRF tienden a cometer más errores para identificar a mujeres, adultos mayores, personas de color, personas transgénero y no binarias<sup>27</sup>.

24 <https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=S>

25 <https://www.theverge.com/2020/3/4/21164482/london-metropolitan-police-face-scanning-consent-civil-liberties>

26 <https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals>

39. El SRF utilizado en la Ciudad Autónoma de Buenos Aires presenta estas mismas ineficiencias. Desde la implementación del sistema en abril de 2019 hasta mediados de julio la herramienta produjo 1227 alertas de las cuales solo 226 quedaron detenidas, es decir un 18% del total<sup>28</sup>. El resto de las notificaciones no tenían requerimientos judiciales que implicarán una detención o fue producto de un error del sistema o de la base de datos. En adición a la tasa de efectividad determinada por la parte demandante en base a información pública y a cuyos detalles nos remitimos, existen notorios casos de afectación a personas inocentes de los cuales mencionamos solo algunos:
  - a. En agosto de 2019, Guillermo Federico Ibarrola fue erróneamente identificado como prófugo por el SRF, estuvo detenido 6 días y casi es trasladado a un penal a pesar de ser inocente<sup>29</sup>.
  - b. María Raquel Holway fue retenida el miércoles 10 de julio de 2019 por una causa iniciada por su expareja de la cual fue sobreseída<sup>30</sup>.
  - c. Una mujer fue erróneamente detenida por 24 hs. por su parecido con una prófuga que había cometido fraude habitacional en 2011<sup>31</sup>.
40. Sin embargo, aún si estos sistemas, especialmente el de la Ciudad Autónoma de Buenos Aires, lograsen mejorar su precisión, erradicar los falsos positivos, y tener bases de datos actualizadas, el problema es aún mayor. Para entender por qué estos sistemas implican una flagrante violación a los Derechos Humanos nos remitimos a lo explicado en la presente intervención en la Sección VII.
41. Una de las razones esgrimidas por el Gobierno de la Ciudad para adoptar el SRF es mejorar la seguridad pública. Sin embargo, no existe ningún estudio (público o privado) que demuestre que las ciudades que implementan estas tecnologías hayan logrado reducir la tasa de criminalidad. Por el contrario, si existe evidencia de uso abusivo<sup>32</sup> y de implementación poco transparente de los sistemas de reconocimiento facial.

## **VII. IMPACTO EN LOS DERECHOS HUMANOS DE LOS SISTEMAS DE RECONOCIMIENTO FACIAL**

42. Los sistemas de reconocimiento facial han sido ampliamente criticados en todo el mundo en especial por su interferencia con los derechos humanos. Entre los derechos que afecta se encuentran:
43. Impacto sobre la **privacidad**: la tecnología de reconocimiento facial con fines de identificación, como explicamos previamente, procesa información biométrica de toda persona que pase frente a sistemas de vigilancia. Es, por lo tanto, una modalidad de

27 <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>

28 [https://www.clarin.com/policiales/identificaron-14-personas-dia-reconocimiento-facial-81-quedo-libre\\_0\\_O\\_WhA1FAf.html](https://www.clarin.com/policiales/identificaron-14-personas-dia-reconocimiento-facial-81-quedo-libre_0_O_WhA1FAf.html)

29 <https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien>

30 [https://tn.com.ar/sociedad/sistema-de-reconocimiento-facial-retuvieron-por-error-una-referente-de-la-lucha-contra-la\\_977335/](https://tn.com.ar/sociedad/sistema-de-reconocimiento-facial-retuvieron-por-error-una-referente-de-la-lucha-contra-la_977335/)

31 <https://www.nueva-ciudad.com.ar/notas/201905/40692-los-errores-del-sistema-de-reconocimiento-facial-detuvieron-a-una-mujer-por-su-parecido-con-una-profuga.html>

32 <https://www.flawedfacedata.com/>

vigilancia masiva. La privacidad, tal cual se encuentra consagrada en la Constitución Nacional, Artículo 18, constituye una de las máximas garantías de la libertad individual frente al abuso del poder imponiendo límites concretos a la potestad punitiva del Estado. Dado que el bien jurídico protegido es la expectativa de privacidad de los individuos, la tutela reposa en la privacidad de las personas y se extiende tanto al domicilio como a aquellos casos en los que cualquier interferencia pudiera afectarla, si se realiza sin el consentimiento de quien sufre la intromisión, inclusive los espacios públicos.

44. En 2013 un conjunto de organizaciones de derechos humanos elaboraron 13 principios a los fines de determinar si determinada tecnología de vigilancia resulta necesaria y proporcional<sup>33</sup>. Dichos principios se encuentran sustentados en el derecho internacional de los derechos humanos y las decisiones de los tribunales internacionales de derechos humanos que han interpretado tales leyes. Esto incluye la jurisprudencia de la Corte Interamericana de Derechos Humanos que interpreta la Convención Americana sobre Derechos Humanos. De acuerdo a tales principios, la tecnología de reconocimiento facial con fines de seguridad pública no es necesaria por cuanto existen otros mecanismos que no implican la constante intromisión a la intimidad de los transeúntes para cumplir con el objetivo para los cuales fueron diseñados. Tampoco es proporcional en tanto que la sensibilidad de la información a la que accede el sistema y la gravedad de la infracción sobre los derechos humanos es excesiva en relación al objetivo que persigue.
45. Impacto sobre la **libertad de expresión**: de acuerdo al Artículo 13 de la Constitución Nacional, “No se puede restringir el derecho de expresión por vías o medios indirectos,... por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones”. El reconocimiento facial se constituye justamente en una restricción por cuanto el hecho de estar bajo constante vigilancia puede generar un efecto inhibitorio y desincentivar fuertemente la disidencia pacífica, sobre todo de aquellas personas críticas de las autoridades que tienen el control de estas tecnologías.
46. Impacto sobre la **libertad de reunión y asociación**: la tecnología de reconocimiento facial puede dificultar de forma significativa el derecho de reunión pacífica y asociación al eliminar el anonimato e impedir el libre ejercicio de estos derechos por el miedo a futuras represalias<sup>34</sup>. Consagrado en el Artículo 15 de la Constitución Nacional este derecho ha sido esencial para el avance de nuestra democracia, por lo que requiere de una especial protección y que cualquier restricción esté debidamente justificada. La experiencia internacional, indica que esta tecnología ha sido uno de los mayores

33 <https://necessaryandproportionate.org/es/principios/>

34 En Julio de 2020, Access Now publicó el reporte “Defensa de la libertad de reunión pacífica y asociación en la era digital: bajas de contenido, apagones de Internet y vigilancia” donde entre otras temáticas se analiza el impacto de las tecnologías de reconocimiento facial sobre este derecho.

<https://www.accessnow.org/nuevo-desorden-mundial-ataques-digitales-a-la-libertad-de-reunion-pacifica-y-asociacion/>

impedimentos a la hora de permitir manifestarse libremente al pueblo. Casos ejemplificativos los encontramos en Rusia<sup>35</sup>, India<sup>36</sup> y Hong Kong<sup>37</sup>.

47. Impacto sobre el **derecho a la protección de los datos personales**: uno de los problemas más graves de los sistemas de reconocimiento facial es que para su funcionamiento deben recolectar datos biométricos de los transeúntes. De acuerdo a la ley argentina de protección de datos personales, Ley 25.326, a la resolución 4/2019 de la Agencia de Acceso a la Información Pública, al Convenio 108 y a los proyectos de reforma de la ley de protección de datos personales, no cabe duda que los datos biométricos son datos sensibles. Incluso, de las capturas de las cámaras para obtener los datos biométricos pueden inferirse otros datos sensibles como la raza e incluso la religión. Debido al potencial discriminatorio y al daño que implica un uso abusivo o ilegítimo de los mismos, los datos sensibles cuentan con una protección especial (Artículo 7, Ley 25.326).
48. Para recolectar o procesar datos sensibles la única base de legitimidad es el consentimiento de los y las titulares de los datos. En el caso de los SRF, las personas que transitan frente a las cámaras no están en conocimiento de que sus datos biométricos están siendo procesados. Para evitar la recolección forzada de estos datos, las personas solo cuentan con la alternativa de evitar transitar por las zonas donde se encuentran las cámaras, lo cual implica una afectación a su **derecho a la libertad de circulación**.
49. Es fundamental comprender además que, a diferencia de otros datos personales sensibles, como las contraseñas o las claves de seguridad, una persona no puede cambiar su rostro si se hace un mal uso de la información captada o esta resulta comprometida.
50. Impacto sobre el **derecho a la no discriminación**: como ha sido explicado previamente, se ha demostrado que esta tecnología tiene dificultades para distinguir personas de tez oscura<sup>38</sup>, lo cual deriva en un sinnúmero de falsos positivos y afecta de forma desproporcionada a grupos que ya se encuentran en situación de vulnerabilidad.
51. Impacto sobre la **presunción de inocencia y debido proceso**: la tecnología de reconocimiento facial con fines de identificación asume que todas las personas son sospechosas hasta tanto se analizan sus datos biométricos y descarte que la persona no es a quien se busca, vulnerando así la presunción de inocencia y el debido proceso.
52. Impacto sobre el **derecho a un recurso efectivo**: la tecnología de reconocimiento facial menoscaba este derecho ya que es posible que las personas no sepan dónde han sido captados sus rostros, y aunque lo sepan y deseen impugnar, generalmente no existen mecanismos y procesos para hacerlo.

35 <https://www.reuters.com/article/russia-protests-tech/fears-raised-over-facial-recognition-use-at-moscow-protests-idUSL8N2KA54T>

36 <https://www.reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ>

37 <https://www.nytimes.com/es/2019/07/31/espanol/reconocimiento-facial-hong-kong.html>

38 <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>

## VIII. CASOS DE PROHIBICIÓN DE LOS SISTEMAS DE RECONOCIMIENTO FACIAL

53. A diferencia de lo que sucede en la Ciudad Autónoma de Buenos Aires, la tendencia en países democráticos es la prohibición de estas tecnologías cuando son utilizadas por fuerzas de seguridad justamente por su desproporcionada interferencia con los derechos humanos. Por el contrario, los países con tendencias autoritarias expanden su utilización<sup>39</sup>.
54. Entre 2019 y 2020, múltiples ciudades y estados de los Estados Unidos de América han prohibido su uso:
- a. En Octubre de 2019, el gobernador del Estado de California, Gavin Newsom, firmó oficialmente un proyecto de ley que impone una moratoria sobre el uso del reconocimiento facial por parte de las fuerzas del orden durante tres años<sup>40</sup>. Otras municipalidades de dicho estado prohibieron su uso: San Francisco<sup>41</sup>, Berkeley<sup>42</sup>, Oakland<sup>43</sup> y Alameda<sup>44</sup>.
  - b. Estado de Massachusetts las ciudades de Easthampton<sup>45</sup>, Boston<sup>46</sup>, Springfield<sup>47</sup>, Cambridge<sup>48</sup>, Northampton<sup>49</sup>, Brookline<sup>50</sup> y Somerville<sup>51</sup> también la prohibieron.
  - c. En septiembre de 2020, la ciudad de Portland del Estado de Oregon prohibió el uso de tecnología de reconocimiento facial por parte de los órganos públicos de la ciudad, incluida la policía local, así como de las empresas orientadas al público, como tiendas, restaurantes y hoteles<sup>52</sup>.
  - d. La ciudad de Portland del Estado de Maine no solo prohibió el uso de la tecnología por parte de las fuerzas policiales sino que además dispuso que los y las ciudadanas tienen derecho a reparación en caso de que se viole la prohibición<sup>53</sup>.
55. El 21 de junio de 2021, las dos agencias de privacidad de la Unión Europea (UE), la Junta Europea de Protección de Datos (EDPB) y el Supervisor Europeo de Protección de Datos (EDPS), pidieron que se prohíba el uso del reconocimiento facial en espacios

39 <https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/>

40 <https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215>

41 <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>

42 <https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recognition-1839087651>

43 <https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php>

44 <https://ebcitizen.com/2019/12/23/alameda-approves-facial-recognition-technology-policy-ban-will-seek-ordinance/>

45 <https://www.aclum.org/en/news/easthampton-passes-municipal-ban-face-surveillance-technology>

46 <https://www.aclum.org/en/news/boston-becomes-largest-city-east-coast-ban-face-surveillance>

47 <https://www.aclum.org/en/news/springfield-passes-municipal-moratorium-face-surveillance-technology>

48 <https://www.aclum.org/en/news/cambridge-passes-municipal-ban-face-surveillance-technology>

49 <https://www.aclum.org/en/news/northampton-bans-government-face-surveillance>

50 <https://www.aclum.org/en/news/brookline-bans-municipal-use-face-surveillance>

51 <https://www.aclum.org/en/news/somerville-city-council-moves-ban-government-face-surveillance>

52 <https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html>

53 <https://www.theverge.com/2020/11/4/21536892/portland-maine-facial-recognition-ban-passed-surveillance>

públicos. Según su entendimiento, la prohibición de esta tecnología “es el punto de partida necesario si queremos preservar nuestras libertades y crear un marco legal para la IA centrado en el ser humano”<sup>54</sup>.

56. En agosto de 2020, el Tribunal de Apelación de Gales del Sur encontró que el uso de la tecnología de reconocimiento facial por parte de la Policía viola los derechos de privacidad, las leyes de protección de datos y las leyes de igualdad<sup>55</sup>. De acuerdo al tribunal, la implementación del sistema no tuvo en cuenta el potencial discriminatorio, es violatorio del derecho a la igualdad y que el procesamiento de los datos sensibles se encuentra en oposición al derecho a la protección de los datos personales.
57. La tendencia a la prohibición de los SRF también se encuentra en el sector privado. En junio de 2020, IBM<sup>56</sup>, Amazon<sup>57</sup> y Microsoft<sup>58</sup> anunciaron que dejarían de ofrecer sus productos de reconocimiento facial a las fuerzas policiales y de seguridad.

## IX. POSICIÓN DE ORGANISMOS INTERNACIONALES

58. Organismos regionales e internacionales también se han expresado en contra del uso de las tecnologías de reconocimiento facial por parte de las fuerzas públicas.
59. El 13 de septiembre de 2021, el **Consejo de Derechos Humanos en su Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y el Secretario General, referido al “Derecho a la Privacidad en la Era Digital”**<sup>59</sup>, analiza “cómo el uso generalizado por los Estados y las empresas de la inteligencia artificial, incluida la elaboración de perfiles, la toma de decisiones automatizada y las tecnologías de aprendizaje automático, afecta el disfrute del derecho a la privacidad y los derechos asociados.”
60. De acuerdo al reporte, “el reconocimiento biométrico remoto en tiempo real plantea serias preocupaciones en virtud del derecho internacional de los derechos humanos... El reconocimiento biométrico remoto está vinculado a una profunda interferencia con el derecho a la privacidad. La información biométrica de una persona constituye uno de los atributos clave de su personalidad, ya que revela características únicas que la distinguen de otras personas. Además, el reconocimiento biométrico remoto aumenta drásticamente la capacidad de las autoridades estatales para identificar y rastrear sistemáticamente a las personas en los espacios públicos, lo que socava la capacidad de las personas para vivir sin ser observadas y tiene como resultado un efecto negativo directo en el ejercicio de los derechos a la libertad de expresión, de reunión pacífica y de asociación, así como la libertad de circulación. En este contexto, la Alta

54 <https://www.reuters.com/technology/eu-privacy-watchdogs-call-ban-facial-recognition-public-spaces-2021-06-21/>

55 <https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/>

56 <https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/>

57 <https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition>

58 <https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/>

59 [https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A\\_HRC\\_48\\_31\\_AdvanceEditedVersion.docx](https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx)

Comisionado acoge con satisfacción los recientes esfuerzos para limitar o prohibir el uso de tecnologías de reconocimiento biométrico en tiempo real.”

61. El reporte concluye que “Un enfoque de la legislación y la regulación proporcional al riesgo requerirá la prohibición de ciertas tecnologías de IA, aplicaciones o casos de uso, donde crearían impactos potenciales o reales que no están justificados por el derecho internacional de los derechos humanos, incluidos aquellos que no superen las pruebas de necesidad y proporcionalidad. Además, no deben permitirse los usos de la inteligencia artificial que estén intrínsecamente en conflicto con la prohibición de la discriminación... Dado que puede tomar tiempo antes de que se puedan evaluar y abordar los riesgos, los Estados también deberían imponer moratorias al uso de tecnología potencialmente de alto riesgo, como el reconocimiento facial remoto en tiempo real, hasta que se garantice que su uso no puede violar los derechos humanos”.
62. Posterior a la publicación del reporte, la Alta Comisionada para los Derechos Humanos de Naciones Unidas, Michelle Bachelet, en conferencia de prensa dijo que los países deberían prohibir el uso de aplicaciones de Inteligencia Artificial que no cumplan con leyes internacionales de derechos humanos. En dicha oportunidad la Comisionada expresó su preocupación sobre el "nivel sin precedentes de vigilancia en todo el mundo por parte de actores estatales y privados", que insistió era "incompatible" con los derechos humanos<sup>60</sup>.
63. En el **Informe Anual de la Comisión Interamericana de Derechos Humanos de 2020, el Relator Especial para la Libertad de Expresión, Pedro Vaca Villareal**, expresó que “La Relatoría nota con preocupación la aprobación por parte de la legislatura de la Ciudad Autónoma de Buenos Aires de un sistema de reconocimiento facial, que prevé la instalación de sistemas de videovigilancia a cargo de las autoridades de la Ciudad... Pese a la advertencia de diversas organizaciones de la sociedad civil, la iniciativa fue aprobada sin debatirse en la Comisión de Derechos Humanos y Garantías, tal como lo habían solicitado.”<sup>61</sup>
64. Como ya hemos mencionado previamente, en su visita al país, el **Relator Especial sobre el derecho a la privacidad, Joseph Cannataci** criticó extensamente el uso del SRF en la Ciudad Autónoma de Buenos Aires. Entre otras observaciones adicionales a las previamente citadas, debemos destacar las siguientes observaciones:
  - a. “Durante mi visita, he observado una falta general de confianza en los servicios de inteligencia de Argentina. Posiblemente debido a la historia reciente de Argentina, a una fuerte cultura de opacidad y a algunos casos de vigilancia ilegal muy publicitados, muchas personas en Argentina sospechan que están personalmente bajo vigilancia y que los agentes de inteligencia actúan sin supervisión ni vigilancia.”
  - b. “Soy consciente de la necesidad de detener a las personas sospechosas de haber cometido delitos y llevarlas ante la justicia, pero no veo la proporcionalidad de instalar una tecnología con graves implicaciones para la privacidad para buscar en una lista de 46.000 personas que actualmente incluye a menores y delitos no graves y que no se actualice y compruebe cuidadosamente su exactitud.”

60 [https://www.washingtonpost.com/politics/un-urges-moratorium-on-use-of-ai-that-imperils-human-rights/2021/09/15/a706e96a-1618-11ec-a019-cb193b28aa73\\_story.html](https://www.washingtonpost.com/politics/un-urges-moratorium-on-use-of-ai-that-imperils-human-rights/2021/09/15/a706e96a-1618-11ec-a019-cb193b28aa73_story.html)

61 <https://www.oas.org/es/cidh/docs/anual/2020/capitulos/rele.PDF>

- c. “Los funcionarios y funcionarias a los que entrevisté dijeron que estaban seguros de que el derecho a la privacidad no estaba siendo violado por los sistemas existentes y que cumplían los requisitos legales, pero que no podían explicar su necesidad y proporcionalidad. En estos y otros casos similares es esencial que las evaluaciones preliminares de impacto se lleven a cabo inmediatamente y sin demora y que sus recomendaciones sobre salvaguardias y recursos se cumplan de inmediato.”

## **X. CAMPAÑAS DE SOCIEDAD CIVIL**

- 65. En conjunción con las decisiones estatales de prohibir las tecnologías de reconocimiento facial, de las empresas de discontinuar su desarrollo y de las declaraciones de organismos internacionales en su contra, las organizaciones de la sociedad civil han desarrollado numerosas campañas para combatir estas tecnologías. Entendemos estas iniciativas esenciales para comprender la unidad en las posiciones de las distintas partes interesadas en relación a los peligros que implica el uso de esta tecnología por parte de las fuerzas policiales y de seguridad.
- 66. De igual forma, numerosas organizaciones de la sociedad civil a nivel local e internacional abogan por la prohibición de esta tecnología. A continuación haremos mención de las campañas desarrolladas y nos remitiremos a sus contenidos para mayor información:
  - a. Access Now. Campaña “BanBS”<sup>62</sup>. Carta abierta que pide una prohibición mundial de las tecnologías de reconocimiento biométrico que permiten una vigilancia masiva y discriminatoria.
  - b. Coalición de organizaciones europeas, “Reclaim Your Face”<sup>63</sup>. Iniciativa de la sociedad civil para solicitar a la Comisión Europea la prohibición de las prácticas biométricas de vigilancia masiva.
  - c. Internet Freedom Foundation, India. Campaña “Project Panoptic”<sup>64</sup>. Iniciativa para promover la transparencia y la rendición de cuentas de las partes interesadas gubernamentales relevantes involucradas en el despliegue e implementación de proyectos de tecnología de reconocimiento facial (FRT) en la India.
  - d. Amnistía Internacional. Campaña “Ban The Scan”<sup>65</sup>. Iniciativa para solicitar a la ciudad de Nueva York que prohíba el uso del reconocimiento facial por parte de agencias gubernamentales.
  - e. Asociación por los Derechos Civiles. Campaña “ConMiCaraNo”<sup>66</sup>. Campaña de concientización sobre los riesgos de los sistemas de reconocimiento facial desplegados en la Argentina.

62 <https://www.accessnow.org/ban-biometric-surveillance/>

63 <https://reclaimyourface.eu/>

64 <https://panoptic.in/about>

65 <https://banthescan.amnesty.org/>

66 <https://conmicarano.adc.org.ar/>



## **XI. CONCLUSIÓN**

67. Solicitamos respetuosamente se nos reconozca como intervinientes en el presente proceso por haber probado nuestro interés legítimo para tal efecto y en consecuencia, se sirva V.S. conceder la razón a la parte demandante atendiendo, entre otras, las razones que fueron expuestas anteriormente y que pueden resumirse así::
- a. La base de datos sobre la cual contrata los datos biométricos al ser defectuosa afecta derechos fundamentales de personas inocentes;
  - b. Los datos recolectados por las cámaras son datos sensibles (incluso de menores de edad) obtenidos de forma ilegítima al no requerir el consentimiento de los y las transeúntes de acuerdo a las normas de protección de datos personales y a tratados internacionales en la materia;
  - c. No están garantizadas las medidas de seguridad necesarias para el procesamiento, conservación y eliminación de tales datos;
  - d. No se han cumplido con los estándares y normas de transparencia y rendición de cuentas;
  - e. La empresa desarrolladora del software de reconocimiento facial, NTechLab cuenta con antecedentes de haber facilitado violaciones a los derechos humanos;
  - f. No hubo etapa consultiva con las múltiples partes interesadas previa a la adquisición e implementación de la tecnología y previa a la aprobación de la Ley 1686-D-2020;
  - g. No se llevó a cabo una evaluación de impacto de la privacidad y de los datos personales;
  - h. Ha quedado comprobada la alta tasa de ineficiencia del sistema de reconocimiento facial implementado lo cual afecta a personas inocentes;
  - i. No existen pruebas de que su implementación mejore la seguridad pública;
  - j. Incluso si mejorase su efectividad, esto representaría aún mayores riesgos para los derechos humanos;
  - k. La tecnología afecta de forma innecesaria y desproporcionada a derechos consagrados en la Constitución Nacional y en Tratados Internacionales de los cuales Argentina es firmante, a saber: privacidad, libertad de expresión, libertad de reunión y asociación, protección de los datos personales, libertad de circulación, no discriminación, presunción de inocencia, debido proceso y recurso efectivo;
  - l. El uso de esta tecnología por parte de las fuerzas policiales y de seguridad ha sido prohibida en numerosos países democráticos mientras se ha expandido en los países con regímenes tendientes al autoritarismo;
  - m. Empresas líderes de tecnología como Amazon, IBM y Microsoft han decidido no continuar con estos desarrollos por su interferencia en los derechos humanos;
  - n. Numerosos organismos internacionales han recomendado su prohibición;
  - y
  - o. Organizaciones de la sociedad civil a nivel internacional, regional y local coinciden en que la única alternativa es su prohibición;

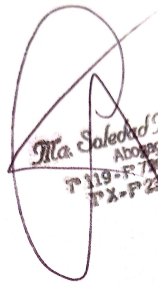
XII. PETITORIO:

Por lo expuesto solicito:

1-Se me tenga por presentado en calidad de amicus curiae y por constituido el domicilio procesal y electrónico.

2-Se declare la admisibilidad del amicus curae.

PROVEER DE CONFORMIDAD  
SERÁ JUSTICIA



Ma. Soledad Marín  
Abogada  
T 119-R 7160 CAS.  
TX-P 230 CAS.



PETER R. MICEK

21 OCT. 2021

I.D. 165 571 257

(New York State)



**Poder Judicial**  
Ciudad de Buenos Aires

Leyenda: 2021 - Año del Bicentenario de la Universidad de Buenos Aires

Tribunal: JUZGADO N°2 - CAYT - SECRETARÍA N°3

Número de CAUSA: EXP 182908/2020-0

CUIJ: J-01-00409611-4/2020-0

Escrito: SE PRESENTAN EN CALIDAD DE AMICUS CURIAE

Con los siguientes adjuntos:  
documental acces2.pdf

FIRMADO ELECTRONICAMENTE 12/10/2021 21:44:25

MARINARO MARIA SOLEDAD - CUIL 27-23004423-1