#### SE PRESENTA EN CALIDAD DE AMICUS CURIAE.

Señor Juez:

Sebastián Pilo (CPACF T° 104, F° 494, CUIT 20-29544405-4), en mi carácter de apoderado de la Asociación Civil por la Igualdad y la Justicia (en adelante, "ACIJ"), con el patrocinio letrado de María Guillermina Greco (T°124 F°518) y Marcelo Alejandro Giullitti Oliva (CPACF T° 136, F° 657), en los autos caratulados "OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.) c/ Gobierno de la Ciudad Autónoma de Buenos Aires s/ amparo" (exp. n° 182908/2020-0), constituyendo domicilio procesal en Av. de Mayo 1161, piso 1°, oficina "1" de la Ciudad Autónoma de Buenos Aires (Zona 55) y domicilio electrónico en la CUIT 27-35348598-4, a Ud. me presento y digo:

#### I. OBJETO

En el carácter invocado, vengo a solicitar que admita el presente memorial de *amicus curiae*. En él, se brindarán argumentos relacionados con la inconstitucionalidad e ilegalidad de los sistemas basados en el reconocimiento facial, en ocasión de su implementación en el ámbito de la Ciudad Autónoma de Buenos Aires. Se expondrán las razones por las cuales la utilización de dichas tecnologías resultaría lesiva de derechos constitucionales, en particular del derecho a la igualdad y no discriminación (art. 16 CN), y a la privacidad e intimidad (arts. 18 y 19 CN). A su vez, se citarán casos análogos que evidencian las problemáticas legales que el uso de este tipo de sistemas ha provocado en otros países.

La finalidad de esta presentación, en consecuencia, es acercar al tribunal argumentos basados en el derecho constitucional, en el derecho internacional de los derechos humanos y en nuestra experiencia como asociación civil, que permitan evaluar las políticas implementadas desde la perspectiva de los derechos humanos, profundizar en ciertas cuestiones que consideramos de vital importancia, revertir la

situación denunciada y afianzar al Poder Judicial en su rol de garante de la supremacía constitucional.

Cabe destacar que ACIJ no ha recibido financiamiento ni ayuda económica de ninguna de las partes, ni asesoramiento en cuanto a los fundamentos de la presentación. El resultado del proceso tampoco representa para esta organización ningún tipo de beneficio patrimonial directo o indirecto.

En virtud de la relevancia de las cuestiones que se debaten en el caso, el interés que tiene ACIJ en torno a ellas y de su trayectoria en la materia, solicitamos que esta presentación sea formalmente admitida.

#### II. PERSONERÍA

La Asociación Civil por la Igualdad y la Justicia se encuentra autorizada para funcionar con carácter de persona jurídica conforme a la Resolución nº 231/03 de la Inspección General de Justicia, de fecha 12 de marzo de 2003. Se acompañan a este escrito copia de dicha resolución y copias del Acta Fundacional y Estatuto de ACIJ.

Por otra parte, soy apoderado de ACIJ, de acuerdo con lo que surge de la copia simple del poder general administrativo y judicial que adjunto y que declaro bajo juramento vigente en todos sus términos.

## III. INTERÉS DE ACIJ EN EL CASO

ACIJ es una organización civil apartidaria, sin fines de lucro, dedicada a la defensa de los derechos de los grupos más desfavorecidos de la sociedad y al fortalecimiento de la democracia en Argentina. Tiene por objetivos defender la efectiva vigencia de la Constitución Nacional, los principios del Estado de derecho, promover el cumplimiento de las leyes que protegen a los grupos desaventajados y la

erradicación de toda práctica discriminatoria, y contribuir al desarrollo de prácticas participativas y deliberativas de la democracia.

En este caso particular, se encuentran controvertidos derechos reconocidos por la Constitución Nacional que se vinculan directamente con el trabajo de ACIJ, por ser esenciales para alcanzar un sistema democrático robusto, en el que se respeten plenamente los derechos humanos. En primer lugar, se halla en juego el derecho a la igualdad y no discriminación, que ilumina y atraviesa la totalidad de los programas temáticos que históricamente han formado parte de nuestra organización. En efecto, hace años trabajamos para erradicar toda política y toda práctica que conduzca a discriminar directa o indirectamente a colectivos vulnerabilizados, como los niños, niñas y adolescentes, las personas con discapacidad y las personas que viven en barrios populares. Por otro lado, en el caso se halla en juego el derecho a la intimidad y a la privacidad, ambos fundamentales para la plena vigencia del Estado de derecho y para el fortalecimiento de las instituciones democráticas, finalidades que también integran la misión de la asociación<sup>1</sup>.

#### IV. FUNDAMENTOS DE LA PRESENTACIÓN DEL AMICUS CURIAE

En nuestra práctica jurídica se encuentra aceptado e incorporado el instituto del *amicus curiae*, de conformidad con los antecedentes existentes en el derecho comparado y en el derecho internacional de los derechos humanos. El *amicus curiae* es una figura procesal reconocida por una vasta cantidad de tribunales nacionales e internacionales, que permite traer a un proceso judicial argumentos y opiniones de terceros ajenos a él, a fin de clarificar criterios y aportar estándares sustanciales para la resolución de la disputa.

Se trata de una figura clásica, con antecedentes en el Derecho Romano, que fue incorporada paulatinamente a la práctica judicial de tradición anglosajona desde el

<sup>&</sup>lt;sup>1</sup> Puede accederse a más información sobre nuestro trabajo ingresando a <a href="https://acij.org.ar/">https://acij.org.ar/</a>

siglo IX. Hoy en día, pasó a ser de aprovechamiento habitual a nivel internacional, y es reconocida por diferentes organismos internacionales.

En tal sentido, no debemos perder de vista que la actuación de los Amigos del Tribunal tiene sustento a nivel regional en el Sistema Interamericano, desde que fue objeto de regulación en el Reglamento de la Corte Interamericana de Derechos Humanos (art. 62.3), y expresamente autorizada por la Comisión Interamericana de Derechos Humanos, en base a lo establecido en los arts. 44 y 48 de la Convención Americana sobre Derechos Humanos.

La aceptación de esta figura a nivel nacional encuentra su fundamento, aun con anterioridad a la reforma de 1994, en lo dispuesto en el art. 33 de la Constitución Nacional, en la medida en que los fines que inspiran dicha participación conjugan sustancialmente las dos coordenadas que dispone el texto: la soberanía del pueblo y la forma republicana de gobierno.

Respecto de la importancia de este tipo de presentaciones se ha dicho que "...La posibilidad de fundar decisiones judiciales en argumentos públicamente ponderados constituye un factor suplementario de legitimidad de la actuación del Poder Judicial. La presentación del amicus curiae apunta entonces a concretar una doble función: a) aportar al tribunal bajo cuyo examen se encuentra una disputa judicial de interés público argumentos u opiniones que puedan servir como elementos de juicio para que aquél tome una decisión ilustrada al respecto; y b) brindar carácter público a los argumentos empleados frente a una cuestión de interés general decidida por el Poder Judicial, identificando claramente la toma de posición de los grupos interesados, y sometiendo a la consideración general las razones que el tribunal tendrá en vista al adoptar y fundar su decisión".<sup>2</sup>

.

<sup>&</sup>lt;sup>2</sup> Abregú, M. y Courtis, C., "Perspectivas y posibilidades del amicus curiae en el derecho argentino", transcripto en *La aplicación de los tratados sobre derechos humanos por los tribunales locales*, compilado por los nombrados, CELS, Editores del Puerto, Buenos Aires, 1997, p. 388.

La existencia de un Estado de derecho trae aparejada la necesidad de permitir a diferentes organizaciones civiles presentarse espontáneamente en todos los juicios que versen sobre la vigencia de los derechos humanos. Es por ello que, incluso antes de que se regulara el instituto, los tribunales argentinos se inclinaron por su admisibilidad en múltiples ocasiones. A modo de ejemplo, en la causa nro. 761, sobre "Hechos ocurridos en el ámbito de la Escuela Superior de Mecánica de la Armada", la Cámara Federal en lo Criminal y Correccional de la Capital Federal en pleno resolvió admitir un memorial en derecho presentado por dos organizaciones internacionales de derechos humanos, CEJIL y Human Rights Watch/Americas, que lo hicieron a los efectos de ofrecerle argumentos sobre la obligación del Estado para con los y las familiares de las víctimas de desaparición forzada.

Cabe recordar que en la causa "Provincia de San Luis v. Estado Nacional y otros" del año 2003, con anterioridad al dictado de la acordada 28/2004, la Corte Suprema de Justicia de la Nación (en adelante, "Corte Suprema" o "CSJN") señaló que "la Corte, en el ámbito de la propuesta conciliatoria en la que estaba ocupada, consideró conveniente oír a las asociaciones bancarias involucradas, viabilizando así la intención de esas entidades de no mantenerse ajenas a un conflicto generalizado que ya había sido expresada en la causa M.12XXXVIII 'Ministerio de Economía y Banco Central de la República Argentina s/ apelación contra medidas cautelares'. En consecuencia citó a una nueva audiencia y convocó a la Asociación de Bancos Argentinos -ABA-, a la Asociación de Bancos Públicos y Privados de la República Argentina -ABAPRA- y a las partes en este proceso para que concurrieran a ese acto..." (Fallos 326:417, cfr. consid. 7°).

Es decir que la Corte Suprema también reconoció expresamente que, con base en las amplias facultades instructorias que le concede el art. 36 del Código Procesal Civil y Comercial de la Nación, se encuentra facultada a escuchar la opinión de

entidades que no son parte en el proceso, pero pueden aportar una opinión autorizada para la solución del caso.

Como se adelantó, la admisibilidad de esta forma de participación en procesos judiciales se ve consolidada a partir de la incorporación del derecho internacional al ámbito del derecho interno, sobre todo desde el año 1994, con la jerarquización de ciertos instrumentos de derechos humanos. Concretamente, los tribunales tuvieron en cuenta que esta figura se encuentra comprendida en el art. 44 de la Convención Americana sobre Derechos Humanos y en los reglamentos de la Corte Interamericana de Derechos Humanos.

En igual sentido, se ha dicho que toda vez que "[e]l Reglamento de la Corte Interamericana, a su vez, establece en forma expresa en su art. 54.3 la posibilidad de presentarse en calidad de amicus curiae ante dicho tribunal (...) resulta entonces absurdo prohibir a instituciones o grupos interesados presentarse en calidad de amicus curiae ante los tribunales internos -oportunidad frente a la que el Estado tiene posibilidades de remediar la alegada violación en sede interna- y conceder esa posibilidad después "3".

Refuerza esta argumentación la regulación expresa de la posibilidad de presentar *amicus curiae* ante la CSJN mediante el dictado de la acordada 28/2004, pues resultaría irrazonable que este instituto se admitiera ante el Máximo Tribunal y se rechazara en instancias inferiores.

A través de la mencionada acordada, la Corte Suprema reconoció expresamente que terceros ajenos a las partes que cuenten con una reconocida competencia sobre la cuestión debatida y demuestren un interés inequívoco en la resolución final del caso, pueden presentarse en las causas que tramitan ante sus

<sup>&</sup>lt;sup>3</sup> Abregú, M. y Courtis, C., "Perspectivas y posibilidades del amicus curiae en el derecho argentino", en *La aplicación de los tratados sobre derechos humanos por los tribunales locales*, Editores del Puerto, Madrid, 2004.

estrados en las que se ventilen cuestiones de trascendencia institucional o que resulten de interés público, a fin de ofrecer argumentos relevantes para la decisión del asunto. En sus considerandos, el tribunal sostuvo que el *amicus* estaba destinado a permitir la participación ciudadana en la administración de justicia, y agregó que "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" (cfr. consid. 2°).

Allí se consideró que la intervención de *amicus* también halla su fundamento en lo dispuesto en el art. 33 de la Constitución, y que "la actuación de los Amigos del Tribunal encuentra sustento en el sistema interamericano al cual se ha asignado jerarquía constitucional (art. 75, inc. 22), pues ha sido objeto de regulación en el Reglamento de la Corte Interamericana de Derechos Humanos (art. 62.3) y ha sido expresamente autorizada por la Comisión Interamericana de Derechos Humanos con sustento en los arts. 44 y 48 de la Convención Americana" (cfr. consid. 2°).

Más cerca en el tiempo, la Corte Suprema dejó dicho, en la Acordada 7 del año 2013, que el propósito perseguido con la intervención de nuevos actores como Amigos del Tribunal es pluralizar y enriquecer el debate constitucional, así como fortalecer la legitimidad de las decisiones jurisdiccionales dictadas por este tribunal en cuestiones de trascendencia institucional.

El reglamento sobre la Intervención de los Amigos del Tribunal que surge del art. 1 de la Acordada 7/13 de la CSJN 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". Además, en su art. 4 establece que "la actuación del Amigo del Tribunal tiene por objeto enriquecer la deliberación en cuestiones Institucionalmente relevantes...", como consideramos que es el caso traído a colación. El art. 13 prevé, a su vez, que las opiniones o sugerencias del Amigo del Tribunal tienen por objeto ilustrar a la Corte Suprema, y que, si bien no vinculan a esta, pueden ser tenidas en cuenta en su pronunciamiento.

En conclusión, en cuestiones de gran trascendencia e impacto público, los tribunales consideran admisible la presentación de *amicus curiae*, fundamentando dicha posición en diversas normas fundamentales y principios constitucionales. De ese modo, admiten y promueven la participación ciudadana en los procesos judiciales, escuchando a una mayor cantidad de voces que enriquecen el debate, lo que fortalece la legitimidad democrática de sus decisiones.

De esta manera, y dadas las cuestiones puestas en debate en estos autos, consideramos oportuno y por demás ventajoso el aporte de argumentos que nutran la discusión, siempre en resguardo del interés ciudadano, la plena vigencia de los derechos humanos y el fortalecimiento de las instituciones democráticas.

#### V. FUNDAMENTOS DE DERECHO

- 1. La utilización del reconocimiento facial vulnera el derecho a la igualdad y no discriminación
  - a. El diseño y la implementación de un software de reconocimiento facial resulta discriminatorio

La discriminación ocurre cuando una persona es tratada de forma menos favorable a otra que se encuentra en la misma situación, en razón de poseer determinadas características individuales que le son inherentes, como la raza, el sexo u otras prohibidas por los tratados internacionales de derechos humanos.<sup>4</sup>

Partiendo de ese concepto, cabe afirmar que el diseño y la implementación de los programas de reconocimiento facial conduce a situaciones de discriminación debido a sesgos en la programación del algoritmo, o como resultado de su manejo por parte de individuos o autoridades de los programas gubernamentales.

En lo referido al diseño, los sistemas de reconocimiento facial funcionan mediante la comparación de características biométricas de dos rostros. Para poder realizar esta tarea, deben aprender cuándo se trata de la misma persona y cuándo no. Esto se logra a partir de una base de datos de distintas caras. La tecnología en cuestión funciona en base a probabilidades. El sistema ofrece un porcentaje de acierto en relación al parecido de la persona identificada con aquella a la que se busca. Este resultado nunca será del 100%, por lo cual quien implemente el sistema debe decidir qué porcentaje considera aceptable<sup>5</sup>.

Dado que las bases de datos para el entrenamiento de estas tecnologías suelen componerse predominantemente por hombres blancos cisgénero<sup>6</sup>, los sistemas de reconocimiento aprenden mejor cómo diferenciar a personas con estas características que al resto de la población. El resultado es que **la mayoría de estos programas** presentan sesgos en cuanto a la utilización de criterios de distinción basados en

ulares.pdf (fecha de consulta: 25 de octubre de 2021).

https://www.theregreview.org/2021/03/20/saturday-seminar-facing-bias-in-facial-recognition-technology/

<sup>&</sup>lt;sup>4</sup> Saba, R., "Igualdad de trato entre particulares" en Revista Lecciones y Ensayos Nro. 89, Facultad de Derecho de la Universidad de Buenos Aires, 2011, p. 230, disponible en: <a href="http://www.derecho.uba.ar/publicaciones/lye/revistas/89/saba-roberto-p-igualdad-de-trato-entre-partic">http://www.derecho.uba.ar/publicaciones/lye/revistas/89/saba-roberto-p-igualdad-de-trato-entre-partic</a>

<sup>&</sup>lt;sup>5</sup> Asociación por los Derechos Civiles, "Avanza la Regulación del Reconocimiento Facial en la Legislatura Porteña", 18 de septiembre de 2020, disponible en: <a href="https://adc.org.ar/2020/09/18/avanza-la-regulacion-del-reconocimiento-facial-en-la-legislatura-portena/">https://adc.org.ar/2020/09/18/avanza-la-regulacion-del-reconocimiento-facial-en-la-legislatura-portena/</a> (fecha de consulta: 14 de octubre de 2021).

<sup>&</sup>lt;sup>6</sup> Ver al respecto:

el sexo, edad y etnia de las personas, categorías consideradas sospechosas por el derecho internacional de los derechos humanos. Por ejemplo, se ha sostenido que estos sistemas son menos precisos en mujeres y personas racializadas que en hombres blancos.<sup>7</sup> Asimismo, existen altas posibilidades de sesgo racial que son reproducidas por quienes los programan, y que causan que el algoritmo funcione en forma discriminatoria<sup>8</sup>.

Existen numerosos casos de errores del sistema, lo que determina que se registren altos índices de falsos positivos o negativos, que llevan a diferentes tipos de discriminación sobre diversos grupos poblacionales. En los casos en los que estos sistemas se utilizan para realizar detenciones, podrían conducir a detener personas inocentes, lo que alteraría la presunción de inocencia, pues la persona detenida debería acreditar que no es quien el sistema dice que es. De hecho, se han detectado algunos donde ciertas personas fueron detenidas en razón de tener "rasgos similares" a la persona que se buscaba. 10

Adicionalmente, el diseño del sistema requiere de la carga de datos, que puede presentar también errores humanos. Por ejemplo, en julio de 2019, una mujer titular de una ONG y militante social fue detenida en la estación Retiro en razón de que hayan cargado su DNI por error en el sistema.<sup>11</sup> Otro caso tuvo lugar en 2019, cuando un hombre fue identificado por el sistema al pasar por una estación de

<sup>&</sup>lt;sup>7</sup> Ibíd.

<sup>&</sup>lt;sup>8</sup> Schlesinger, A., O'Hara, K. P., & Taylor, A. S.. Let's Talk About Race. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, 2018, disponible en: https://sci-hub.se/10.1145/3173574.3173889 (fecha de consulta: 13 de diciembre de 2021).

<sup>&</sup>lt;sup>9</sup> Buolamwini, J. y Timnit G., "Gender shades: Intersectional accuracy disparities in commercial gender classification", en Conference on fairness, accountability and transparency, 2018, pp. 77-91, disponible en: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (fecha de consulta: 11 de diciembre de 2021).

<sup>&</sup>lt;sup>10</sup> Ibid.

<sup>&</sup>lt;sup>11</sup> Todo Noticias, "De un DNI mal cargado a una cara parecida: las víctimas del sistema de reconocimiento facial en Buenos Aires", 23 de julio de 2019, disponible https://tn.com.ar/policiales/de-un-dni-mal-cargado-una-cara-parecida-las-victimas-del-sistema-de-reco nocimiento-facial-en-buenos 980528/ (fecha de consulta: 7 de octubre de 2021)

subte. La Policía de la Ciudad lo detuvo por tres horas, y finalmente se comprobó que se trataba de un error en la carga de los datos de una persona prófuga.<sup>12</sup>

El Comité de Naciones Unidas para la Eliminación de la Discriminación Racial publicó en noviembre de 2020 la Recomendación General Nº 36,<sup>13</sup> una guía para combatir los prejuicios raciales entre las policías de todo el mundo, enfatizando, entre otras cuestiones, el grave riesgo del sesgo algorítmico cuando se utiliza la inteligencia artificial (IA) en la aplicación de la ley.

Los expertos y expertas del Comité sostienen que el mayor uso de los macrodatos, la inteligencia artificial, el reconocimineto facial y otras nuevas tecnologías por parte de las fuerzas de seguridad aumentan el riesgo de profundizar la discriminación racial, la xenofobia y, en consecuencia, la violación de derechos humanos. En el considerando 12 de la Recomendación 36/2020, este organismo expresa que "la utilización cada vez mayor de nuevas herramientas tecnológicas, incluida la inteligencia artificial, en ámbitos como la seguridad, el control de fronteras y el acceso a los servicios sociales, puede profundizar el racismo, la discriminación racial, la xenofobia y otras formas de exclusión".

El uso de tecnologías de reconocimiento facial incrementa la posibilidad de que se realicen perfiles raciales, lo cual da lugar a la adopción de decisiones discriminatorias, ya que, tal como sostiene el mencionado Comité "[l]a práctica de la elaboración de perfiles raciales por los agentes del orden viola los principios fundamentales de los derechos humanos, que se basan en: a) la no discriminación

https://www.chequeado.com/investigacion/video-vigilancia-en-buenos-aires-la-otra-cara-del-control/) (fecha de consulta: 21 de octubre de 2021).

<sup>&</sup>lt;sup>12</sup> Chequeado, "Video-vigilancia en Buenos Aires: La otra cara del control", 28 de mayo de 2020, disponible en:

<sup>&</sup>lt;sup>13</sup> Comité de Naciones Unidas para la Eliminación de la Discriminación Racial, Recomendación general núm. 36/2020, relativa a la prevención y la lucha contra la elaboración de perfiles raciales por los agentes del orden, CERD/C/GC/36, 29 de noviembre de 2020.

por razón de raza, color, ascendencia u origen nacional o étnico, u otros motivos interseccionales; y b) la igualdad ante la ley. También puede violar los derechos al debido proceso y un juicio imparcial. Estos principios y derechos son los pilares de la Declaración Universal de Derechos Humanos (arts. 2 y 7) y la Convención (arts. 2 y 5 a)" (consid. 21). En este sentido, Verene Shepard, miembro del Comité, advierte que los datos históricos de arrestos sobre un barrio pueden reflejar prácticas policiales con prejuicios raciales; y estos datos pueden profundizar el riesgo de vigilancia excesiva, lo que a su vez posibilita más arrestos, creando un círculo de retroalimentación peligroso. 14

En el considerando 23 de la citada recomendación se advierte que, según lo establecido en el art. 2 de la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial, cada Estado se ha comprometido a no incurrir en ningún acto o práctica de discriminación racial contra personas, grupos de personas o instituciones, y a velar por que todas las autoridades e instituciones públicas, nacionales y locales, actúen de conformidad con esta obligación. En conjunto con lo establecido en los arts. 5 y 6 de la Convención, los Estados tienen la obligación de asegurarse de que no se apliquen prácticas de elaboración de perfiles raciales a través de la adopción de medidas preventivas.

En síntesis, conforme lo que hasta aquí se ha expuesto, la programación y utilización de softwares de reconocimiento facial trae aparejada la creación de perfilamientos raciales por parte de las fuerzas policiales que las utilizan, a causa de los sesgos discriminatorios que tanto quienes programan los algoritmos como el contenido de las bases de datos generan en el sistema de reconocimiento. Estas deficiencias en la tecnología en cuestión vulneran el derecho a la igualdad y no discriminación de aquellas personas que son señaladas erróneamente por el sistema

\_

<sup>&</sup>lt;sup>14</sup> Noticias ONU, "Cuidado con el algoritmo, puede discriminar, advierten expertos en derechos humanos a la Policía", 26 de noviembre de 2020, disponible en: <a href="https://news.un.org/es/story/2020/11/1484762">https://news.un.org/es/story/2020/11/1484762</a> (fecha de consulta: 14 de octubre de 2021).

con motivo de su sexo, su edad o su etnia, y constituyen una inversión -prohibida- de la carga de la prueba que atenta contra el principio de inocencia.

b. El software de reconocimiento facial produce un impacto desproporcionado sobre ciertos grupos de población en particular

En los hechos, la utilización de este tipo de software produce efectos diferenciales sobre aquellos grupos que se encuentran menos representados en el algoritmo, al hacerlos más propensos a sufrir los errores del mismo. Si bien aún no se ha logrado obtener información certera sobre cómo está "entrenado" este algoritmo en particular (cuestión que es parte del objeto de la causa), sí es posible hacer algunas consideraciones respecto del impacto que este tipo de sistemas han mostrado tener en el mundo para ciertas poblaciones particulares y sobre por qué ello es contrario a nuestro ordenamiento constitucional.

Tal como sostiene la Corte Interamericana de Derechos Humanos, "una violación del derecho a la igualdad y no discriminación se produce también ante situaciones y casos de discriminación indirecta reflejada en el impacto desproporcionado de normas, acciones, políticas o en otras medidas que, aún cuando sean o parezcan ser neutrales en su formulación, o tengan un alcance general y no diferenciado, produzcan efectos negativos para ciertos grupos vulnerables". <sup>15</sup> Este criterio de violación del principio de igualdad por discriminación

noviembre de 2021).

<sup>&</sup>lt;sup>15</sup> Corte Interamericana de Derechos Humanos, Cuadernillo de Jurisprudencia Nº 14: Igualdad y no discriminación, 30 de julio de 2014, disponible en: <a href="https://www.corteidh.or.cr/sitios/libros/todos/docs/cuadernillo14.pdf">https://www.corteidh.or.cr/sitios/libros/todos/docs/cuadernillo14.pdf</a> (fecha de consulta: 27 de

indirecta fue aplicado por el Tribunal en casos como "Artavia Murillo" y en "Caso de personas dominicanas y haitianas expulsadas vs. República Dominicana". <sup>17</sup>

En ese sentido, el uso del algoritmo en cuestión no solo genera que ciertos grupos poblacionales estén en una situación de desventaja por el mero hecho de pertenecer a dicho grupo, sino que también presenta un mayor índice de error cuando se trata de mujeres, <sup>18</sup> personas transgénero o no binarias, niños, niñas y adolescentes <sup>19</sup> y personas racializadas, causando un impacto desproporcionado sobre estos colectivos, tal como explicaremos a continuación.

#### i. Discriminación hacia las mujeres

El reconocimiento facial no es confiable para la correcta identificación de mujeres. En su mayor parte, estos sistemas son entrenados utilizando imágenes de hombres.<sup>20</sup> Las consecuencias de este insuficiente entrenamiento son especialmente claras cuando se trata de mujeres racializadas: el análisis del rendimiento de los sistemas comerciales de clasificación de género de 3 empresas (Microsoft, Face++ e IBM) demuestra que si bien se mostró una clasificación casi perfecta para los hombres blancos (tasas de error del 0% al 0,8%), las tasas de error

<sup>&</sup>lt;sup>16</sup> Corte Interamericana de Derechos Humanos, "Artavia Murillo y otros (Fertilización in Vitro) vs. Costa Rica", sentencia del 28 de noviembre de 2012, disponible en <a href="https://www.corteidh.or.cr/docs/casos/articulos/seriec\_257\_esp.pdf">https://www.corteidh.or.cr/docs/casos/articulos/seriec\_257\_esp.pdf</a> (fecha de consulta: 9 de diciembre de 2021).

<sup>&</sup>lt;sup>17</sup> Corte Interamericana de Derechos Humanos, "Caso de personas dominicanas y haitianas expulsadas Vs. República Dominicana", sentencia del 28 agosto 2014, disponible en: <a href="https://corteidh.or.cr/docs/casos/articulos/seriec\_282\_esp.pdf">https://corteidh.or.cr/docs/casos/articulos/seriec\_282\_esp.pdf</a> (fecha de consulta: 9 de diciembre de 2021).

<sup>&</sup>lt;sup>18</sup> Lehr A. K. y Crumpler W., Facing the risk, Part 1: Mapping the Human Rights Risks in the Development of Facial Recognition Technology, 2021, p. 16, disponible en: <a href="https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210727">https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210727</a> Lehr FacingtheRisk On e 1.pdf?iT5sia0du2 S.L4E1jr63ThOOexITipk (fecha de consulta: 13 de diciembre de 2021).

<sup>&</sup>lt;sup>19</sup> *Ibíd*., p. 17.

<sup>&</sup>lt;sup>20</sup> *Ibid.*, p. 16.

de las mujeres racializadas, específicamente en las mujeres negras, llegaban al 35,5%.<sup>21</sup>

Pero el entrenamiento del algoritmo no es su única falla. En un estudio realizado para la IEEE Transactions on Information Forensics and Security -una importante revista científica publicada por el Institute of Electrical and Electronics Engineers de Nueva York- se puso a prueba el índice de error de tres algoritmos comerciales de reconocimiento facial diferentes en relación a diversos grupos. En los resultados, se demostró que todos y cada uno de ellos tenían un desempeño significativamente peor a la hora de identificar a mujeres que a hombres, teorizando que esto se debía a que a la hora de entrenar dichos algoritmos se hacía mayor foco en exponerlos a imágenes de este último grupo. Sin embargo, al someter a los mismos algoritmos a una nueva prueba, habiendo entrenado de manera igualitaria con imágenes de ambos grupos (120.000 en total), volvió a arrojar el mismo resultado desfavorable. Como conclusión, el estudio demostró con suficiente evidencia una inherente falibilidad del sistema en relación a la identificación de muieres.<sup>22</sup>

#### ii. Discriminación hacia el colectivo LGBTIQIA+

El género es una construcción social de las culturas humanas presente en el mundo físico y virtual. Los algoritmos formados por las tecnologías de reconocimiento facial reflejan los sesgos personales, culturales, históricos y sociales de quienes los crean, por lo que debe señalarse que en su código se encuentran las arbitrarias opiniones sobre el género de quienes lo escriben. Esta tecnología no es

<sup>&</sup>lt;sup>21</sup> Buolamwini, J. y Timnit G., "Gender shades: Intersectional accuracy disparities in commercial gender classification", en *Conference on fairness, accountability and transparency*, 2018, pp. 77-91, disponible en: <a href="https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf">https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf</a> (fecha de consulta: 13 de diciembre de 2021).

<sup>&</sup>lt;sup>22</sup> Klare, B. F., Burge, M. J., Klontz, J. C., Vorder Bruegge, R. W. y Jain, A. K. (2012) "Face Recognition Performance: Role of Demographic Information", en IEEE Transactions on Information Forensics and Security, vol. 7, nro. 6, diciembre de 2012, pp. 1789-1801.

intrínsecamente neutra, sino que es construida por quienes representan solo una parte de la población mundial para ser utilizada sobre cualquier persona del mundo.

Resulta imposible, por lo menos al día de hoy, que los sistemas de reconocimiento facial en uso correctamente identifiquen el género de las personas, en tanto este es un concepto multifacético y primordialmente interno que demuestra fluidez y una mayor diversidad de lo que se puede codificar. Un sistema que solo es entrenado con la binariedad de "hombre" y "mujer" no es compatible con las leyes nacionales y obligaciones internacionales que ha asumido el Estado argentino. El género no es algo que pueda leerse con precisión a través de los rasgos físicos (cara, cuerpo o voz) por parte de los humanos ni de los algoritmos digitales.

En ese sentido, participantes LGBTQIA+ de un estudio sobre género y sistemas de reconocimiento expresaron que temen que estos sistemas sean utilizados, intencionadamente o no, como herramienta para renovar estructuras opresivas que ya afectan a esta comunidad. En el sentido de que se refuerza el binarismo en la concepción del género, se anula la autonomía de los usuarios y usuarias, y se impone una vigilancia que socava su privacidad y seguridad.<sup>23</sup>

Por otra parte, investigadores e investigadoras de la Universidad de Colorado Boulder pusieron a prueba los sistemas de gigantes tales como *IBM*, *Amazon*, *Microsoft* y *Clarifai* con fotografías de hombres transgénero y descubrieron que eran mal identificados como mujeres un 38% de las veces. Mientras que con hombres y mujeres cisgénero (o aquellas que se identificaban con el que habían nacido) se reconocían correctamente un 98.3% y un 97.6% de las veces respectivamente.

<sup>&</sup>lt;sup>23</sup> Hamidi, F., Scheuerman, M. K., y Branham, S. M., "Gender Recognition or Gender Reductionism? The Social Implications of Embedded Gender Recognition Systems", en *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, p. 6.

Además, los algoritmos también fallan en identificar personas que no se reconocen a sí mismas como hombres o mujeres un 100% de las veces.<sup>24</sup>

Un representante del Centro Nacional para la Igualdad Transgénero -una organización sin fines de lucro fundada en Washington en 2003- expresó temor porque dicha tecnología pudiese ser usada para restringir el acceso de personas trans a lugares etiquetados por género, tales como vestidores y baños, por identificarlos erróneamente.<sup>25</sup> El crecimiento del uso de estos sistemas ha dejado muy por detrás a las regulaciones de la ley, ya que no se le ha dado el tratamiento legislativo adecuado y proporcional al impacto que termina por tener en la vida de la ciudadanía en general y de las minorías en particular.

Las organizaciones que luchan por los derechos de las personas LGBTQIA+ se han unido junto a otras treinta organizaciones enfocadas a la defensa de derechos civiles y libertades individuales en una carta abierta liderada por la Unión Estadounidense por las Libertades Civiles, con el fin de demandar al Congreso que sancione el cese de uso de toda tecnología de esta índole para fines policiales y migratorios, en tanto la misma no sea tratada apropiadamente y regulada por ley.<sup>26</sup>

## iii. Discriminación hacia niños, niñas y adolescentes

En septiembre de 2021 el Servicio de Investigación del Parlamento Europeo emitió un informe especializado sobre la regulación de la FRT (Facial Recognition Technology) donde se hace especial hincapié en la preocupación que esta acarrea con

<sup>&</sup>lt;sup>24</sup> Sri Moola Nathan, A., "Top biometric systems fail to ID transgender people", en Biometric Technology Today, vol. 2019, no. 10, p. 11.

<sup>&</sup>lt;sup>25</sup> Chibbaro, L. Jr., "LGBT advocates raise alarm over 'facial recognition' technology", en Washington Blade, 13 de agosto de 2019, disponible en: <a href="https://www.washingtonblade.com/2019/08/13/lgbt-advocates-raise-alarm-over-facial-recognition-technology/?cfchljschltk=pmd\_ecr3495Vx.4JkBsktOsfzOvs541eug7viaNLJykURSO-1635799420-0-gqNtZGzNAqWjcnBszOjR (fecha de consulta: 1 de octubre de 2021).

<sup>&</sup>lt;sup>26</sup> American Civil Liberties Union, Coalition Letter Calling for a Federal Moratorium on Face Recognition, 3 de junio de 2019, disponible en: <a href="https://www.aclu.org/letter/coalition-letter-calling-federal-moratorium-face-recognition">https://www.aclu.org/letter/coalition-letter-calling-federal-moratorium-face-recognition</a> (fecha de consulta: 1 de octubre de 2021).

respecto a los niños, niñas y adolescentes, específicamente teniendo en cuenta que debido a la baja precisión sobre rostros de jóvenes en crecimiento, son los individuos más vulnerables.<sup>27</sup>

De acuerdo con los resultados de la evaluación del National Institute of Standards and Technology (NIST), Human Rights Watch estima que en un ámbito controlado estos algoritmos arrojan seis veces más falsas coincidencias para un niño, niña o adolescente de entre 10 y 16 años que para una persona adulta de entre 24 y 40<sup>28</sup>. Además, los errores son más frecuentes cuanto menor sea la edad. Esto puede deberse a que los algoritmos son entrenados con imágenes de rostros adultos, y además al hecho de que las infancias están en una etapa de crecimiento y cambios físicos.<sup>29</sup>

La niñez y la adolescencia como etapas formativas para la identidad y posibilidades futuras hacen aún más grave los posibles daños que el uso de las tecnologías en cuestión acarrean sobre esta población. La falsa identificación, como posible víctima o persona sospechosa, puede ser profundamente traumática para este grupo.<sup>30</sup> Esta es una realidad aún mayor para las y los jóvenes racializados: en Estados Unidos las y los jóvenes negros tienen 500% más probabilidades de ser detenidos o internados en centros de salud que sus compañeras y compañeros blancos.<sup>31</sup> En este análisis, también debe tenerse en cuenta la mayor vulnerabilidad

\_\_\_

<sup>&</sup>lt;sup>27</sup> Madiega, T. y Mildebrath, H., "Regulation facial recognition in the EU - In-depth analysis" para European Parlament Research Services, 2021, disponible en: <a href="https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS\_IDA(2021)698021\_EN.p">https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS\_IDA(2021)698021\_EN.p</a> df (fecha de consulta: 7 de octubre de 2021).

<sup>&</sup>lt;sup>28</sup> Human Rights Watch, Carta al Lic. Horacio Rodríguez Larreta sobre el Sistema de Reconocimiento Facial de Prófugos y derechos de niñas y niños, 9 de octubre de 2020, disponible en: <a href="https://www.hrw.org/es/news/2020/10/09/carta-al-lic-horacio-rodriguez-larreta-sobre-el-sistema-de-reconocimiento-facial-de">https://www.hrw.org/es/news/2020/10/09/carta-al-lic-horacio-rodriguez-larreta-sobre-el-sistema-de-reconocimiento-facial-de</a> (fecha de consulta: 7 de octubre de 2021).

<sup>&</sup>lt;sup>29</sup> Barrett, L., "Ban Facial Recognition Technologies for Children - And for Everyone Else", en Boston University Journal of Science and Technology Law 26, nro. 2, 5 de septiembre de 2020, p. 247. <sup>30</sup> *Ibid.*, p. 254.

<sup>&</sup>lt;sup>31</sup> Thomas, J. M. & Wilson, M., "The Color of Youth transferred to the adult criminal justice system: policy and practice recommendations 1", National Association of Social Workers: Washington, 2017.

que sufren por no tener control sobre la forma en que sus familias o sus instituciones hacen uso de sus imágenes.

Adicionalmente, el hecho de que espacios transitados por las niñeces y juventudes sean monitoreados por dispositivos de reconocimiento facial tiene la potencialidad de impactar negativamente en su desarrollo, comportamiento y autoestima, partiendo del conocimiento de una efectiva falta de privacidad.<sup>32</sup> Además, los errores que surgen del uso de estas tecnologías por parte de las fuerzas públicas tendrán consecuencias especialmente graves para la seguridad, la libertad y trayectoria vital de niños, niñas y adolescentes.<sup>33</sup>

## iv. Discriminación hacia personas racializadas

En el mes de junio del año 2020, las compañías IBM, Amazon y Microsoft pusieron en pausa y limitaron la venta de su tecnología de reconocimiento facial en Estados Unidos en el contexto de las protestas del movimiento "Black Lives Matter", cuando activistas antirracistas demostraron el rol que cumplía esta tecnología en la perpetuación de la violencia y discriminación racial sistémica como herramienta de las fuerzas de seguridad. Señalados como "anti-black technologies" ("tecnologías anti personas negras"), los sistemas de reconocimiento facial constituyen una particular amenaza a este grupo.

En otros lugares del mundo, se ha comprobado que en la utilización de algoritmos de reconocimiento facial hay un sesgo marcado, ya que presentan más fallas en personas racializadas.<sup>34</sup> Un reciente estudio del National Institute of Standards and Technology (NIST), al evaluar 189 algoritmos de 99 distintos desarrolladores estadounidenses, encontró tasas elevadas de falsos positivos sobre

<sup>&</sup>lt;sup>32</sup> Barrett, L., op. cit., p. 257.

<sup>&</sup>lt;sup>33</sup> *Ibid.*, p. 285.

<sup>&</sup>lt;sup>34</sup> La Capital, "Reconocimiento facial en vía pública: sesgos y prohibiciones en otras ciudades del mundo", 11 de noviembre de 2020, disponible en: <a href="https://www.lacapital.com.ar/la-ciudad/reconocimiento-facial-via-publica-sesgos-y-prohibiciones-otra-s-ciudades-del-mundo-n2622511.html">https://www.lacapital.com.ar/la-ciudad/reconocimiento-facial-via-publica-sesgos-y-prohibiciones-otra-s-ciudades-del-mundo-n2622511.html</a> (fecha de consulta: 27 de noviembre de 2021).

caras de personas asiáticas, negras e indígenas en comparación con caras de personas blancas.<sup>35</sup> Un creciente pero ya establecido cuerpo de investigación sobre algoritmos de reconocimiento facial<sup>36</sup> muestra divergentes porcentajes de error sobre distintos grupos demográficos, encontrando los peores resultados sobre mujeres negras de entre 18 y 30 años.<sup>37</sup> Aquí surge un peligro de utilización acrítica e irreflexiva de tecnologías usualmente señaladas por contener sesgos raciales.<sup>38</sup>

El riesgo de discriminación de personas racializadas resulta más alto aún en contextos que involucran a las fuerzas de seguridad.<sup>39</sup> Particularmente, la utilización de bases de datos obtenidas por las fuerzas de seguridad a partir de fotos de identificación, incorpora al algoritmo sesgos raciales propios del sistema judicial (en este caso, argentino)<sup>40</sup>, amplificándolos con la tecnología de vigilancia del siglo XXI.

Aun en el caso hipotético de que exista un algoritmo especialmente entrenado con una base de datos diversa, la configuración predeterminada de las cámaras digitales no está optimizada para capturar de manera efectiva los tonos de piel "no

\_

<sup>&</sup>lt;sup>35</sup> National Institute of Standards and Technology, "Study Evaluates Effects of Race, Age, Sex on Face Recognition Software", 2019, disponible en <a href="https://perma.cc/A3CD-K624">https://perma.cc/A3CD-K624</a> (fecha de consulta: 14 de octubre de 2021).

<sup>&</sup>lt;sup>36</sup> Furl, N., Phillipa, J. y O'Toole, A., "Face recognition and the other-race effect: computational mechanisms for developmental contact hypothesis", en Cognitive Science, vol. 26, nro. 6, 2002, pp. 797-815.

<sup>&</sup>lt;sup>37</sup> Klare, B.F, Burge, M., Klontz, J.C., Vorder Bruegge, R. W, y Jain, A. K., "Face Recognition Performance: Role of Demographic Information", en IEEE Transactions on Information Forensics and Security, vol. 7, nro. 6, 2012, p. 1798.

<sup>&</sup>lt;sup>38</sup> Najibi, A., "Racial discrimination in face recognition technology", en Harvard GSAS Science Policy Group - Special edition: Science Policy and social justice, 2020, disponible en: <a href="https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/">https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/</a> (fecha de consulta: 1 de noviembre de 2021).

<sup>&</sup>lt;sup>39</sup> Amnistía Internacional, "Ban dangerous facial recognition technology that amplifies racist policing", 27 de enero de 2021, disponible en: <a href="https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/">https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/</a>) (fecha de consulta: 1 de noviembre de 2021).

<sup>&</sup>lt;sup>40</sup> Por ejemplo, ver: Corte Interamericana de Derechos Humanos, "Caso Acosta Martines y otros vs. Argentina", sentencia del 31 de agosto de 2020, párrs. 37-40.

caucásicos" o más oscuros. 41 Tales imágenes tomadas para la creación de bases de datos no se ajustan necesariamente a la verdadera apariencia de la persona. La captura de estas imágenes es muy deficiente, requiriendo del desarrollo de prácticas compensatorias y mejoras tecnológicas para subsanar. Esto resulta en bases de datos de pobre calidad para el reconocimiento de personas racializadas.

## 2. La implementación de un software de reconocimiento facial vulnera el derecho a la privacidad e intimidad

Los derechos a la privacidad y a la intimidad están previstos en los arts. 18 y 19 de nuestra Constitución Nacional. Por su parte, el art. 12 de la Declaración Universal de los Derechos Humanos establece que "[n]adie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación y que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". De esta misma manera remarca la protección el Pacto Internacional de Derechos Civiles y Políticos en su art. 17 y la Convención Americana sobre Derechos Humanos en el segundo y tercer párrafo de su art. 11.

En el ámbito de la Ciudad de Buenos Aires, la Ley N° 1.845 regula "el tratamiento de datos personales referidos a personas físicas o de existencia ideal, asentados o destinados a ser asentados en archivos, registros, bases o bancos de datos del sector público de la Ciudad de Buenos Aires, a los fines de garantizar el derecho al honor, a la intimidad y a la autodeterminación informativa" (art. 1). La ley funciona como un medio de reglamentación en resguardo de la intimidad de las personas y de sus derechos personalísimos. Al mismo tiempo, funciona como un modo de limitación al poder del propio Estado, ya que establece prohibiciones a la potestad regulatoria estatal.

<sup>&</sup>lt;sup>41</sup> Roth, L.,. "Looking at Shirley, the Ultimate Norm: Colour Balance, Image Technologies, and Cognitive Equity", en Canadian Journal of Communication, vol. 34 nro. 1, 2009, pp. 111-136.

Dicha norma define a los datos personales como aquella información de cualquier tipo referida a personas físicas o de existencia ideal, determinadas o determinables; y, luego, a los datos sensibles como aquellos datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio a su titular.

En este sentido, tal como se observó en los párrafos anteriores, el software permite recolectar información que sería considerada como "dato sensible", en tanto permite revelar origen étnico o racial y otras características físicas que posibilitarían un trato discriminatorio. La biometría utiliza lo que las personas son para identificarlas, ya que los sistemas biométricos actúan sobre sus cuerpos, lo que deviene aún más grave si consideramos que los datos se recolectan y se utilizan sin su consentimiento. El sistema de reconocimiento facial puede escanear los rostros de cada persona que transite un determinado lugar y el dato biométrico que surge de la captura del rostro resulta ser un identificador tan único de cada individuo como lo es el ADN o la huella dactilar que se almacena y utiliza, al menos, para el entrenamiento del software en cuestión.

Respecto de los datos sensibles, la ley establece la prohibición general de obligar a una persona a proporcionarlos. Asimismo, dispone que solo pueden ser tratados cuando medien razones de interés general autorizadas por ley, y también con finalidades estadísticas o científicas, siempre y cuando no puedan ser identificados sus titulares. Finalmente, prohíbe la formación de archivos, registros, bases o bancos de datos que almacenen información que directa o indirectamente revele datos sensibles, salvo que la ley disponga expresamente lo contrario o que medie el consentimiento libre, previo, expreso, informado y por escrito de quien sea su titular.

Estas dos últimas cláusulas deben ser interpretadas en forma restrictiva, por lo cual, quien utilice o realice bases de datos que contengan datos sensibles, debe demostrar la razonabilidad y la proporcionalidad de la medida.

En ese sentido, la aplicación de un sistema de reconocimiento facial utiliza medios lesivos de los derechos humanos, por cuanto recurre a datos biométricos y al procesamiento de datos sensibles, lo que redunda en una intromisión a la intimidad de toda persona que circule frente a las cámaras de detección. En simples palabras, perjudica los derechos de millones de personas a cambio de la probabilidad -de por sí baja por la población delictiva en sí- de detectar algún transeúnte como un posible prófugo. La irrazonabilidad y desproporcionalidad de la medida resultan patentes en este caso.

A su vez, la recolección de los rasgos faciales mediante este tipo de sistemas se hace en muchos casos sin el consentimiento de las personas, sin que tengan conocimiento de lo que está sucediendo y sin un motivo identificado.<sup>42</sup> En este sentido, el sistema tampoco cumple con lo previsto en el art. 8, inc. 3 de la ley.

Sumado a esta falta de consentimiento, también existen serios riesgos en el almacenamiento y seguridad de la información recolectada. En un caso similar, se produjo una filtración masiva de bases sobre los documentos de identidad y datos biométricos de más de sesenta mil personas<sup>43</sup>, demostrando la falta de protocolos de seguridad para su manejo adecuado.

En el caso que nos ocupa, tal como se viene desarrollando, tampoco existe información respecto de que haya un control suficiente del almacenamiento de

<sup>&</sup>lt;sup>42</sup> Ferreyra, E., "Reconocimiento facial en el espacio público de CABA y los peligros para los derechos humanos", La Ley, Buenos Aires, 2020.

<sup>&</sup>lt;sup>43</sup> Ver, al respecto:

https://www.clarin.com/tecnologia/filtracion-renaper-difunden-datos-sensibles-60-000-argentinos-pide n-cerca-17-mil-dolares-dni 0 2eE kXXBo.html (fecha de consulta: 28 de noviembre de 2021).

# información biométrica de las personas que son captadas por las cámaras que permita contrarrestar los riesgos mencionados.

En la misma línea, en el seno de la Unión Europea se ha previsto la protección al derecho de intimidad, en tanto el derecho a la protección de datos de carácter personal es un derecho fundamental garantizado en el art. 8, primer apartado, de la Carta de los Derechos Fundamentales de la Unión Europea y el art. 16, primer apartado, del Tratado de Funcionamiento de la Unión Europea. También se ha pedido su prohibición dentro del continente europeo, por parte del Comité Europeo para la Protección de Datos, que fundamentó su petición declarando que "el uso de tecnologías de reconocimiento remotos basados en datos biométricos en lugares públicos implicaría el final del anonimato en esos espacios" y que "la aplicación de sistemas de reconocimiento facial atenta abiertamente contra derechos y libertades fundamentales".<sup>44</sup>

El Relator Especial sobre el Derecho a la Privacidad de las Naciones Unidas sostuvo en mayo de 2019 lo siguiente: "Me preocupa que ni Buenos Aires ni Comodoro Rivadavia hayan realizado ninguna evaluación de impacto en la privacidad antes de implementar amplias redes de cámaras de vigilancia o sistemas de reconocimiento facial y reconocimiento de matrículas. 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

https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-feat ures-publicly-accessible\_en (fecha de consulta: 7 de octubre de 2021).

<sup>&</sup>lt;sup>44</sup> European Data Protection Board, "EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination", 2021, disponible en:

impacto se lleven a cabo inmediatamente y sin demora y que sus recomendaciones sobre salvaguardias y recursos se cumplan de inmediato". 45

Se ha argumentado también que el uso de procesos de reconocimiento facial a través de cámaras de video en espacios públicos podría interferir directamente con la libertad de opinión, lo cual también conlleva efectos adversos considerables hacia el derecho a la privacidad, libertad de expresión, y reunión pacífica de acuerdo a un reporte del Consejo de los Derechos Humanos de las Naciones Unidas. Además, las personas que circulan en la Ciudad de Buenos Aires que no quieran que el Estado intervenga en su vida de esta manera o recolecte sus datos personales, disponen como única alternativa evitar reunirse o circular por esos espacios públicos, lo que traería aparejado la afectación de otros derechos, como la libertad de circulación y de reunión.

#### 3. Implementación de sistemas similares en otros países

Los sistemas de reconocimiento facial han despertado alertas y cuestionamientos en otros países del mundo.

A modo de ejemplo, en el mes de mayo del año 2019, la ciudad de San Francisco, una de las más modernas y vanguardistas de los Estados Unidos, se convirtió en la primera dentro del territorio estadounidense en oponerse a esta práctica debido al uso por parte de las fuerzas policiales y otras agencias.<sup>47</sup> La principal motivación tras esta decisión fue la creciente inquietud de la ciudadanía

<sup>&</sup>lt;sup>45</sup> Declaración a los medios de comunicación del Relator Especial sobre el derecho a la privacidad, al concluir su visita oficial a la Argentina del 6 al 17 de mayo de 2019.

<sup>&</sup>lt;sup>46</sup> Reporte de la Alta Comisionada por los Derechos Humanos, "New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States" del 25 de junio de 2020, disponible en: <a href="https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=E">https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=E</a> (fecha de consulta: 7 de octubre de 2021).

<sup>&</sup>lt;sup>47</sup> The New York Times, "San Francisco Bans Facial Recognition Technology", 14 de mayo de 2019, disponible en:

https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (fecha de consulta: 28 de noviembre de 2021).

ante el posible abuso del sistema, así como el rechazo a un posible estado de vigilancia opresivo.

En Portland, ciudad del estado de Oregon, ya se encuentra vigente la más amplia prohibición al uso público y privado de tecnologías de reconocimiento facial en todo Estados Unidos. El ayuntamiento responsable de esta medida justificó la ordenanza en casos documentados de sesgo de género y racial en la tecnología de reconocimiento facial, señalando específicamente que las comunidades marginadas habían sido objeto de sobrevigilancia, sufriendo un impacto dispar y perjudicial por su uso.<sup>48</sup>

El Parlamento Europeo, a través de la resolución A9-0232/2021, adoptó una posición profundamente restrictiva respecto del uso de estas tecnologías por parte de las fuerzas de seguridad, afirmando que debía limitarse, y en algunos casos prohibirse, la utilización de inteligencia artificial y el software de reconocimiento facial para la vigilancia masiva. Con especial preocupación por el uso de herramientas de reconocimiento facial basadas en la inteligencia artificial, el Parlamento afirma que "identifican erróneamente a los grupos étnicos minoritarios, a las personas LGBTI+, a las personas mayores y a las mujeres en mayor proporción, lo que es especialmente preocupante en el contexto de la aplicación de la ley y el Poder Judicial". 49 Sobre el uso de vigilancia masiva que utiliza datos biométricos. incluido el reconocimiento facial, los parlamentarios parlamentarias expresaron que para respetar la privacidad y la dignidad humana debe prohibirse el reconocimiento automatizado de personas en espacios públicos, y que para asegurar el cumplimiento de los derechos

<sup>&</sup>lt;sup>48</sup> Ver, al respecto: <a href="https://www.portland.gov/code/34/10">https://www.portland.gov/code/34/10</a> y <a href="https://www.portland.gov/code/34/10">https://www.portland.gov/code/34/10</a> (fecha de consulta: 28 de noviembre de 2021).

<sup>&</sup>lt;sup>49</sup> Committee on Civil Liberties, Justice and Home Affairs, Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI), 13 de julio de 2021, disponible en: <a href="https://www.europarl.europa.eu/doceo/document/A-9-2021-0232\_EN.html">https://www.europarl.europa.eu/doceo/document/A-9-2021-0232\_EN.html</a> (fecha de consulta 20 de diciembre de 2021).

fundamentales, los algoritmos deben ser transparentes, rastreables y estar suficientemente documentados.

Es importante tener en cuenta también las palabras de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos, Michelle Bachellet, que se expresó en junio de 2020 sobre el tema, declarando: "Ahora más que nunca, mientras personas en todo el mundo se unen para protestar contra el racismo, incluyendo aquel dentro de las fuerzas policiales, el derecho a reunirse pacíficamente jamás ha sido más importante. El reconocimiento facial no debería ser puesto en uso en el contexto de protestas pacíficas sin las salvaguardas esenciales necesarias para garantizar su transparencia, la protección de datos, y supervisión". <sup>50</sup>

La falta de transparencia respecto de la tecnología de reconocimiento facial y su uso resulta preocupante, y sumado a la falta de estándares de control, configura una fuerte amenaza a las libertades individuales. En general no hay suficientes procesos de control de calidad o mecanismos de supervisión del uso de estas tecnologías y de las bases de datos por parte de las fuerzas de seguridad, permitiendo que posibles errores no se detecten ni se corrijan. Los sistemas de Inteligencia Artificial deben ser probados continua, interseccionalmente (a través del tiempo y el espacio, haciendo foco en diferentes culturas, lugares y periodos históricos) y con participación de los colectivos potencialmente afectados por su uso, a fin de descubrir sus deficiencias y enmendarlas, lo que no se ha asegurado en el caso bajo análisis.

Más recientemente, el Parlamento Europeo ha votado a favor de una regulación que prohíbe el uso de sistemas de reconocimiento facial por parte de las fuerzas

.

<sup>&</sup>lt;sup>50</sup> Pronunciamiento completo disponible en: <a href="https://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=F.Un">https://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=F.Un</a> (fecha de consulta: 28 de noviembre de 2021).

<sup>&</sup>lt;sup>51</sup> Barrett, L., *op.cit.*, p. 247.

policiales.<sup>52</sup> Entre los fundamentos de la resolución, el Parlamento expresó que el uso de Inteligencia Artificial por parte del sector de seguridad acarrea riesgos varios, tales como toma de decisiones aleatorias, discriminación, intrusión sobre la privacidad, y entorpecimiento a los sistemas de protección de datos personales, dignidad humana, y la libertad de expresión e información. Dicho organismo declaró que los riesgos de estos sistemas son agravados en los sectores correspondientes a las fuerzas policiales y justicia criminal, ya que pueden afectar directamente al principio de presunción de inocencia, el derecho fundamental a la libertad, a la integridad personal, al debido proceso, y a un juicio justo.<sup>53</sup>

Además de instar a la prohibición de los sistemas de reconocimiento facial, la resolución también ha exhortado a que dicha prohibición se extienda al uso policial de cualquier otra forma de análisis automático de rasgos humanos, tales como huellas digitales, ADN, voz y cualquier otro tipo de signos inherentes a la persona.

Al aprobar esta norma, el Parlamento Europeo expresó su preocupación por los servicios de reconocimiento facial tales como Clearview AI, una base de datos con más de tres billones de fotos que han sido recolectadas ilegalmente desde las redes sociales y otras partes del internet. Según datos de Georgetown Law, Center on Privacy & Technology, una de cada dos personas adultas estadounidenses están en una base de datos de las fuerzas de seguridad que utiliza el reconocimiento facial.<sup>54</sup>

A pesar de que la resolución no es vinculante, ha sido emitida al mismo tiempo que la Unión Europea se encuentra trabajando en nuevas leyes respecto al uso de

53 11 /

<sup>&</sup>lt;sup>52</sup> Committee on Civil Liberties, Justice and Home Affairs, Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 13 de julio de 2021, disponible en: <a href="https://www.europarl.europa.eu/doceo/document/A-9-2021-0232\_EN.html?">https://www.europarl.europa.eu/doceo/document/A-9-2021-0232\_EN.html?</a> (fecha de consulta: 9 de diciembre de 2021).

<sup>53</sup> Ibíd

<sup>&</sup>lt;sup>54</sup> Garvie, C., Bedoya, A. y Frankle, J., "The Perpetual Line-Up: Unregulated Police Face Recognition in America", en Georgetown Law, Center on Privacy & Technology, 2016, disponible en: <a href="https://www.perpetuallineup.org/findings/deployment">https://www.perpetuallineup.org/findings/deployment</a> (fecha de consulta: 13/12/2021).

Inteligencia Artificial, tanto dentro del sector público como el privado; por lo que es de esperar que en el transcurso del siguiente año esta entidad vuelva a expresarse sobre el tema.

#### VI. PETITORIO

Por todo lo expuesto, solicitamos:

- a. Se tenga a la Asociación Civil por la Igualdad y la Justicia por presentada en calidad de *amicus curiae*, y por constituido el domicilio legal denunciado.
- b. Se declare la admisibilidad formal del presente *amicus curiae* y se tenga por presentado.
- c. Se tengan en cuenta las consideraciones que aquí se formulan al momento de decidir en la presente causa.

Proveer de conformidad,

SERÁ JUSTICIA.

**~** 

M. GUILLERMINA GRECO MARCELO A. GIULLITTI OLIVA

Abogado

Abogada

T' 124 F' 518, CPACF T° 136, F° 657, CPACF

SEBASTIÁN E. PILO

Apoderado ACIJ



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

Tribunal: JUZGADO N°1 - CAYT - SECRETARÍA N°1

Número de CAUSA: EXP 182908/2020-0

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

Escrito: SE PRESENTA EN CALIDAD DE AMICUS CURIAE.

FIRMADO ELECTRONICAMENTE 22/12/2021 14:37:56

GRECO MARIA GUILLERMINA - CUIL 27-35348598-4