SE PRESENTA COMO AMIGOS DEL TRIBUNAL

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 Juan Carlos Lara, Codirector Ejecutivo y Paula Jaramillo, Directora, actuando conjuntamente en representación legal de la Organización No Gubernamental de Desarrollo, Defensa y Promoción de los Derechos Humanos en el Entorno Digital, **DERECHOS DIGITALES**, con domicilio en Diagonal Paraguay Nº 458, departamento 2, Santiago de Chile, Rol Único Tributario 65.706.580-3, con personalidad jurídica aprobada mediante el Decreto Exento Nº 2030 de 2005 del Ministerio de Justicia de la República de Chile, con fecha 13 de junio de 2005, en los autos caratulados **OBSERVATORIO DE DERECHO INFORMATICO ARGENTINO O.D.I.A**. contra **GCBA** sobre AMPARO - OTROS **Número: EXP 182908/2020-0** ante V.E., decimos:

1. Objeto

Que vengo a presentarme como *amicus curiae* a los fines de exponer la opinión de Derechos Digitales sobre la causa UT SUPRA conforme las siguientes consideraciones de hecho y derecho que se exponen a continuación:

2. Introducción

Este es un caso de amparo colectivo promovido por el Observatorio de Derecho Informático Argentino (O.D.I.A), una Asociación Civil legalmente registrada para ejercer acciones judiciales en carácter colectivo en Argentina, contra el Gobierno de la Ciudad de Buenos Aires (“GCBA”), para se lograr un control de constitucionalidad y convencionalidad de la Resolución Nº 398/MJYSGC/19 y de la Ley Nº 6.339, en cuanto prevén el “Sistema de Reconocimiento Facial de Prófugos” (“SRFP”), modificando la Ley Nº 5.688, artículos 478, 480, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis.

La petición de amparo narra que el 3 de abril de 2019, el Ministro de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires anunció la implementación de un nuevo SRFP, que funcionaría con inteligencia artificial. Con fecha 25 de abril de 2019 mediante la publicación de la Resolución Nº 398/2019 (de ahora en más "Resolución 398") se implementa el sistema sin discusiones ni debates con la población, especialmente sin comprobar si el sistema contribuye a la mejora de la seguridad pública o cómo impacta en el ejercicio de derechos fundamentales a través de una previa evaluación del impacto en la privacidad ("EIP").

Narra incluso que O.D.I.A. presentó un pedido de información a las autoridades con fecha 4 de julio de 2019 (Anexo IV del Amparo) con 77 preguntas destinadas a: (i) conocer cierta información sobre el proceso mediante el cual se licitó el SRFP; (ii) conocer los antecedentes de la Resolución 398 mediante el cual se implementó el sistema; (iii) averiguar si el GCBA contaba con protocolos de seguridad de la información para el sistema; (iv) conocer los resultados del uso del SRFP en estos primeros meses; (v) conseguir copia de cierta documentación importante; (vi) conocer los antecedentes administrativos previos a su implementación; y (vii) cuestiones puntuales acerca del "Pliego de Especificaciones Técnicas del Servicio de Análisis Integral de Video". Afirma la peticionaria que la respuesta a su pedido de información, el 27 de agosto de 2019, fue incompleta, parcial y deficiente, haciendo un análisis pormenorizado de las respuestas.

En resumen, la petición de amparo aporta los siguientes fundamentos legales: (i) Derechos definidos en la Constitución Argentina enumerados en los artículos 14, 14 bis, 18, 19, 33, 43, 75 inc 22; (ii) artículos 14, 16, 18, 34, 36, 38, 39, 61 de la Constitución de la Ciudad Autónoma de Buenos Aires, (iii) en la Opinión Consultiva OC-5/85 de la Comisión Interamericana de Derechos Humanos (CIDH), Derecho a Reunión de Terceros, (vi) Pacto de San José de Costa Rica artículo 7, (v) Pacto de Derechos Civiles y Políticos en sus artículos 4, 5, 7, 9, 14, 17, 20, 21, 24, (vi) Ley Nº 2.145 de la Ciudad Autónoma de Buenos Aires, (vii) Ley Nº 1.845 de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires, (viii) Ley Nº 25.326 de Protección de Datos Personales, (ix)

Convenio 108 del Consejo de Europa, y (x) jurisprudencia y derecho comparado aplicable al caso.

Con fecha 29 de diciembre de 2019 fue dictada la sentencia de primera instancia, Juzgado Nº 11 Secretaría N° 21, que rechazó la acción de amparo *in limine*, por estimar la falta de configuración de un caso o controversia, fundado en cuestionamientos a la legitimidad activa para la presentación de la acción y la materialidad del daño alegado. O.D.I.A interpuso el recurso de apelación para revocación de la resolución apelada, requiriendo también que se diera lugar a la medida cautelar para suspender la aplicación del SRFP.

Con fecha 11 de agosto de 2021, la Sala I de la Cámara de Apelaciones en lo CATyRC dio lugar al recurso de apelación interpuesto para revocar la sentencia de primer grado y remitir los autos para una nueva radicación de las actuaciones para continuar su trámite. Sin adentrarse en el mérito, el Tribunal señaló que la demandante se encontraba legitimada como parte actora en este caso y que la acción “resulta formalmente procedente".

Es de hacer notar que O.D.I.A presentó una ampliación de la demanda, en el 24 de agosto de 2021, para incorporar la denuncia de hechos nuevos relativos a que en fecha 19 de febrero de 2021, el GCBA perfeccionó una Orden de Compra (2900-0943- OC211) con dos finalidades: 1. Servicio de Instalación de Cámara de Video para Sistema de Vigilancia Vial, cuyo costo es de U$D 318.582.04; y 2. Servicio de Instalación de Cámara de Video para Sistema de Vigilancia Vial, cuyo costo es de U$D 304.073.56. Además, informó en esa ocasión que la solicitud de Acceso a la Información Pública estaba siendo apelada por el GBCA, actualmente en trámite en la Sala III de la Cámara de Apelaciones CATyRC, bajo el EXP J-01-00114771-0/2019-0, solicitando la incorporación de dicha causa en la presente como prueba documental por tratar el mismo objeto de esta demanda de amparo.

Finalmente, con fecha de 31 de agosto de 2021, el Juez de 1ª Instancia resuelve ordenar las medidas de difusión y publicidad propias de las acciones colectivas para la presente causa, así como disponer que el traslado al GCBA será evaluado una vez vencido el plazo conferido para que se presenten todos los

interesados. El 10 de septiembre de 2021, el Juez emite Oficio reiterativo, solicitando nuevamente la publicación del Edicto. Con fecha de 16 de septiembre de 2021 fue publicado por tres (3) días en el Edicto en el Boletín Oficial[1] para citar y emplazar por el término de quince (15) días a contar desde la última fecha de su publicación, 20 de septiembre, para que todas las personas que tengan un interés jurídico en el resultado del litigio se presenten en este litigio tanto como actoras o demandadas.

3. Legitimación de Derechos Digitales para efectuar esta presentación

Es pertinente indicar que Derechos Digitales es una organización no gubernamental independiente y sin fines de lucro, con sede principal en Santiago de Chile y con alcance latinoamericano en su trabajo, que se dedica a la defensa y promoción de los derechos fundamentales en el entorno digital, centrando nuestra atención en el impacto sobre estos derechos del uso y la regulación de las tecnologías digitales desde hace más de quince años.

Fundada en 2005, Derechos Digitales cuenta con una vasta experiencia en defensa de los derechos humanos en relación al impacto sobre ellos en el uso de la tecnología. Ello nos ha llevado a participar en instancias locales, regionales y globales en que se discuten distintas políticas públicas, acuerdos y regulaciones que conciernen al despliegue de tecnologías a través de las cuales los Estados ejercitan sus funciones, impactando en el ejercicio de los derechos fundamentales de sus ciudadanas. Más recientemente, Derechos Digitales ha monitoreado y analizado los casos, problemas, riesgos y desafíos del reconocimiento facial en América Latina[2], y la adopción de herramientas de inteligencia artificial, analizando las iniciativas a nivel regional e identificando áreas de mejora bajo principios internacionales existentes y buenas prácticas que respondan de manera más adecuada al contexto local[3].

1 Boletín Oficial de la Ciudad Autónoma de Buenos Aires - Nro 621 (16/09/2021). Recuperado: https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_EDI-OJ-CITACION-PJCBA-JPICAYTN2-27075230-21-6216.pdf
2 https://reconocimientofacial.info/
3 https://ia.derechosdigitales.org/

Nuestro interés por participar en el proceso de autos como amigos de la Corte está dado porque el principal objeto de discusión de la acción se refiere a la legalidad de cara a la normativa constitucional y convencional de protección de derechos humanos vigente de los actos administrativos y legales que dan funcionamiento al SRFP.

En particular, el presente caso presenta especial relevancia para nuestra organización pues brinda la oportunidad de ilustrar la afectación de una multitud de derechos fundamentales identificados en el amparo presentado que contravienen la protección constitucional ofrecida a éstos por la Ciudad de Buenos Aires y el Estado Federal de la Argentina, así como las obligaciones contraídas por este último a nivel internacional en materia de derechos humanos. Se trata de un caso de atención, no solo a nivel local para garantizar la efectiva protección de los derechos de la ciudadanía, sino también de un caso concreto que puede resultar en un importante precedente para la región, y para el sistema Interamericano de protección de los derechos humanos.

En virtud de lo expuesto, solicitamos a la honorable Tribunal ser tenidos como “amigos de la Corte”, con el propósito de someter a su consideración algunos argumentos para la resolución de la acción de control de constitucionalidad y convencionalidad presentada en contra de la Resolución Nº 398/MJYSGC/19 y de la Ley Nº 6.339, en cuanto prevén el SRFP, modificando la Ley Nº 5.688, artículos 478, 480, 484, 490 e incorporando los artículos 480 bis y 490 bis, que consta en expediente 182908/2020-0.

4. Características de la tecnología de reconocimiento facial

El reconocimiento facial automatizado es una tecnología biométrica que permite reconocer e identificar a las personas mediante sus rasgos faciales. Las tecnologías biométricas utilizan las características físicas y de comportamiento propias de cada individuo, con el objetivo de reconocer, autenticar o identificar, de manera automatizada, a una o múltiples personas.

El reconocimiento facial funciona mediante dos componentes: 1) una cámara de

captura de imágenes; y, 2) un software alimentado por un algoritmo (una fórmula de instrucciones) que está entrenado para reconocer rostros e individualizar sus rasgos. Por ejemplo, determinando la distancia entre los ojos, la nariz y los labios que distingue a una persona de otras. Una vez que se realiza el mapeo de los rasgos faciales a través de la captura de imágenes, el software genera una plantilla con la representación matemática para ese rostro único. Esa plantilla es el dato biométrico dentro de la tecnología de reconocimiento facial. Dado que es una forma de informatización de características físicas o corporales, los datos biométricos han sido caracterizados como datos sensibles por las legislaciones de protección de datos más avanzadas del mundo[4].

En Argentina, la Agencia de Acceso a Información Pública (AAIP) definió a los datos biométricos como "datos sensibles", en los Criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley Nº 25.326 de Protección de los Datos Personales (LPDP):

> *"Criterio 4. Datos biométricos - Los datos biométricos son aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única.*
> *Los datos biométricos que identifican a una persona se considerarán datos sensibles (conforme el artículo 2°, Ley N° 25.326) únicamente cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su titular (v.g. datos que revelen origen étnico o información referente a la salud)*[5].

Con la plantilla biométrica, el rostro puede ser leído por una computadora y contrastado con una base de datos en la que previamente se han almacenado un conjunto de rostros. El software puede llevar a cabo una comparación en tiempo real con todos los rostros almacenados en esa base de datos para determinar si una persona se encuentra registrada allí. Se utiliza así el reconocimiento facial para la *identificación* de una persona.

4 Así por ejemplo se contempla en Art. 4 14) y Art. 9 1) del Reglamento General de Protección de Datos de la Unión Europea (GDPR).
5 AAIP, Resolución 4/2019. (13/01/2019). Recuperado: http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318874/res4AAIP.pdf

La biometría conlleva siempre un proceso de probabilidades, por lo que una vez que el software encuentra una potencial coincidencia, arroja un porcentaje que define qué tan probable es que corresponda a algún o algunos individuos dentro de una base de datos. Ningún sistema biométrico, dentro del cual se incluye el reconocimiento facial, es infalible.

Debido a que el software de reconocimiento facial funciona en base a un algoritmo para la detección, mapeo y contraste de los rasgos faciales, es importante conocer cómo fue entrenado ese algoritmo y cuáles son las tasas de error programadas en el software. Estas tasas de error son las que determinan la probabilidad de identificación/verificación de una persona de manera correcta. El entrenamiento del algoritmo define la precisión con la cual podrá reconocer rostros en diversos escenarios. Por ejemplo, ante cambios de luz, fondos con distintos colores o ángulos variados, que pueden incidir en la precisión del reconocimiento. En esta instancia, aspectos sensibles como el tono de piel y la expresión de género de una persona juegan un papel crucial, dado que el software de reconocimiento facial puede ser más o menos sensible en identificarles y por tanto discriminarlas, sea por ejemplo si confunde a una persona con otra por tener rasgos "parecidos" solo por su color de piel,[6] o incluso estigmatizando a las identidades sexogenéricas no binarias o no cisgenéricas[7].

De acuerdo con la precisión del entrenamiento, los sistemas de reconocimiento facial tendrán una mayor o menor tendencia a ser discriminatorios. La decisión sobre el entrenamiento del algoritmo y las tasas de error con la que contará el software biométrico es tanto una cuestión técnica como política. Es por ello que para evitar consecuencias negativas en el ejercicio de derechos fundamentales en su despliegue, se hace indispensable un debate democrático en que la información técnica de sus características y la posibilidad de auditar externamente sus capacidades y limitaciones se encuentre abierta a la

6 "The Perpetual Line-up", 18 de octubre de 2016, disponible en: https://www.perpetuallineup.org/findings/racial-bias

7 "The challenges of using machine learning to identify gender in images", 5 de septiembre de 2019, disponible en: https://www.pewresearch.org/internet/2019/09/05/the-challenges-of-using-machine-learning-to-identify-gender-in-images/

ciudadanía, desde el diseño de la implementación como parte de la política pública, y con posterioridad durante todo su ciclo de uso, favoreciendo la rendición de cuentas de los poderes públicos.

5. Derechos fundamentales afectados por el despliegue de tecnología de reconocimiento facial en la ciudad de Buenos Aires

La tecnología de reconocimiento facial presenta múltiples problemas, que se vuelven aún más graves cuando se utiliza esta tecnología en la vía pública, como es el caso de la implementación por el Ministerio de Justicia y Seguridad de la Ciudad de Buenos Aires (MJSCB).

El reconocimiento facial es una tecnología de vigilancia encubierta: las personas no tienen manera de corroborar que sus datos biométricos están siendo capturados, procesados y almacenados. Esto implica que tampoco pueden prestar su consentimiento para dicho uso. Incluso si se instalan carteles en las zonas donde se encuentran ubicadas las cámaras de vigilancia con reconocimiento facial, la única alternativa que tendrían las personas para que sus datos biométricos no sean recolectados y procesados es evitar transitar por esos espacios.

Como ha sido afirmado por el Informe "La vigilancia y los derechos humanos" del Relator Especial de Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión:

> *"**Las personas señaladas para ser vigiladas sufren interferencias en sus derechos a la privacidad y a la libertad de opinión y de expresión, independientemente de que las actividades de vigilancia tengan éxito o no. No es necesario que la persona vigilada tenga conocimiento de la intrusión, fallida o exitosa, para que la interferencia en su derecho a la privacidad sea completa**. De hecho, por lo general, los gobiernos buscan instrumentos que permitan llevar a cabo la intrusión sin que la persona vigilada tenga conocimiento de ello.*

No obstante, es fundamental considerar esa interferencia como parte de un esfuerzo general para imponer al objetivo una situación determinada. Si se lleva a cabo con fines ilícitos, el intento de imponer la vigilancia —y la operación con éxito— puede utilizarse en un esfuerzo por silenciar la disidencia, sancionar las críticas o castigar la facilitación de información independiente (y castigar también a las fuentes de esa información). Las sanciones tal vez no se apliquen a los objetivos, sino a su red de contactos. En entornos sometidos a una vigilancia ilícita generalizada, las comunidades vigiladas conocen o sospechan de tales actividades, lo que a su vez perturba y restringe su capacidad para ejercer sus derechos a la libertad de expresión, asociación, creencia religiosa, cultura, etc.

En resumen, la interferencia con la privacidad mediante la vigilancia selectiva está diseñada para reprimir el ejercicio del derecho a la libertad de expresión"[8].

En el caso de la Ciudad Autónoma de Buenos Aires, la instalación de las cámaras de reconocimiento facial en la vía pública implica restringir desproporcionadamente de los derechos de libre circulación, de reunión pacífica y de libertad de expresión. La implementación de esta tecnología en la vía pública permite un mayor grado de automatización de la vigilancia masiva, facilitando individualizar y hacer seguimiento preciso de los movimientos de una persona por las zonas geográficas donde se encuentran dichas cámaras. Esto conlleva un efecto de enfriamiento en el uso de los espacios públicos para el ejercicio de derechos fundamentales esenciales para el ejercicio democrático.

La operación del sistema conlleva a la vez la recolección de información que puede ser sumamente sensible sobre hábitos y costumbres, como por ejemplo la religión que profesa una persona o las condiciones y tratamientos de salud que se encuentre realizando, impactando tanto el derecho de protección de datos personales como la intimidad.

Cuando el reconocimiento facial se implementa en bases de datos para la

8Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Informe "La vigilancia y los derechos humanos", presentado al Consejo de Derechos Humanos, A/HRC/41/35, 28 de mayo 2019, párrafo 21, disponible en: https://undocs.org/es/A/HRC/41/35 . Los destacados aquí y en lo sucesivo son nuestros.

identificación de individuos entre una multitud, como ocurre en este caso, se está interfiriendo además con el principio constitucional de presunción de inocencia. Por la misma naturaleza técnica bajo la cual funciona el reconocimiento facial, se trata a todas las personas que transitan frente a la cámara como posibles culpables u ofensores, pudiendo solamente el algoritmo determinar que no son culpables cuando sus rostros sean procesados y descartados por no estar vinculados a las personas en el sistema de Consulta de Rebeldías y Capturas (CONARC).

Por último, la calibración técnica del algoritmo, así como la calidad de los datos utilizados para realizar la identificación,, determinan el nivel de propensión del sistema a generar resultados discriminatorios contra la población evaluada por el mismo. A este respecto, ya en 2019 durante su visita a Argentina, el entonces Relator Especial de las Naciones Unidas sobre el Derecho a la Privacidad, Joseph Canatacci, advertía respecto del CONARC:

1. *“Al 16 de mayo de 2019, contiene una lista de 46.479 personas.*
2. *La lista contiene el nombre y la edad de la persona buscada, los nombres y apellidos del padre y de la madre, el número nacional de identificación (DNI), el tipo de delito por el que son buscados y la institución y autoridad que emite la orden. Aunque el número de identificación podría ser una herramienta importante para que las autoridades lleven a cabo un arresto, no veo cómo podría considerarse necesario divulgar esta información al público.*
3. *La lista contiene personas buscadas no sólo por delitos graves, como la violación, la extorsión o el homicidio, sino también por otros como el robo simple (3.259 expedientes). En 13.703 expedientes (29,5% del total), no hay información sobre el tipo de delito por el que se busca a la persona.*
4. *La lista contiene 61 menores de edad. Es particularmente preocupante que los menores estén incluidos en la base de datos pública, lo que sería difícil de justificar como el interés superior del niño, tal como lo exige la Convención sobre los Derechos del Niño (artículo 3.1), ratificada por la Argentina el 4 de diciembre de 1990. La Convención también reconoce el derecho de todo niño y niña acusado/a de haber infringido la ley penal "a que se respete plenamente su vida privada en todas las etapas del procedimiento" (artículo 40.b.2.vii), lo que sería incompatible con la*

publicidad de las órdenes de detención contra menores.

5. *La base de datos contiene múltiples errores: por ejemplo, dos personas figuran como de 2 y 3 años de edad, buscadas por asalto y robo. Debido a la posible violación del derecho a la privacidad de una persona, debe garantizarse escrupulosamente la exactitud de dicha lista.*
6. *Otra preocupación que he recibido es que la lista no está debidamente actualizada, por lo que las garantías que podrían tener más de una década de antigüedad todavía se encuentran en la base de datos pública. Aunque la base de datos se actualiza todas las mañanas a las 7 a.m. con los datos proporcionados por los tribunales penales de todo el país, no todos los tribunales parecen revisar la información que introducen en la base de datos, lo que da lugar a errores y discrepancias."*[9]

A continuación se examinan en forma más detallada los distintos derechos fundamentales identificados como gravemente afectados en su ejercicio por el SRFP.

5.1. Derecho de reunión pacífica

El derecho de reunión, consagrado en el artículo 15 de la Convención Americana sobre Derechos Humanos[10], protege la congregación pacífica, intencional y temporal de personas en un espacio determinado para el logro de un objetivo común. También se reconoce y protege en el artículo 21 del Pacto Internacional de Derechos Civiles y Políticos[11]. En el mismo sentido lo reconocen los artículos 14 de la Constitución Argentina y 61 de la Constitución de la Ciudad Autónoma de Buenos Aires. El derecho de reunión es no solo indispensable para el ejercicio de los derechos civiles y políticos, para la expresión colectiva de las opiniones, la libre asociación y la vida democrática de las sociedades, sino que es un derecho fundamental para la defensa y

9Canatacci, Joseph. 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, en: https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=S

10La Convención Americana sobre Derechos Humanos fue ratificada por la Ley Nº 23.054, del 1º de marzo de 1984, y tiene jerarquía constitucional en los términos del artículo 75 inciso 22 de la Constitución de la Nación Argentina. Fue ratificada y aceptada la competencia de la Corte el 5 de septiembre de 1984, con una reserva y declaraciones interpretativas.

11El Pacto Internacional de Derechos Civiles y Políticos fue ratificado por el Gobierno argentino el 8 de agosto de 1986, y tiene jerarquía constitucional en los términos del artículo 75 inciso 22 de la Constitución de la Nación Argentina.

protección de otros derechos.

Las tecnologías de vigilancia, y en particular los sistemas de reconocimiento biométrico, afectan y amenazan el libre ejercicio de estos derechos, pues pueden ser utilizadas para identificar a las personas que participan en estas acciones, vulnerando su anonimato y posibilitando su perfilamiento. Tal como señala el borrador revisado de noviembre de 2019 de la Observación General 37 de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre el derecho de reunión pacífica,

> *"**El mero hecho de que las reuniones tengan lugar en público no significa que la privacidad de los participantes no pueda verse infringida, por ejemplo, mediante el reconocimiento facial y otras tecnologías que pueden identificar participantes individuales en una multitud**. Lo mismo ocurre con el control de las redes sociales para obtener información sobre los participantes en reuniones pacíficas. Se deben ejercer un escrutinio y supervisión independientes sobre la recolección de información y de datos personales de aquellos que participen en reuniones pacíficas"* [12].

En este sentido, los derechos de reunión pacífica y de asociación solo pueden enfrentar limitaciones expresamente fijadas por la ley, necesarias para asegurar el respeto a los derechos ajenos o para la protección de la seguridad nacional y el orden público, y proporcionales al fin perseguido.

El monitoreo de las actividades de los ciudadanos, de las organizaciones políticas y sociales, así como el registro, almacenamiento y procesamiento de datos derivados de su actividades, violan los derechos a la libre reunión y asociación, en especial en cuanto afectan a la garantía de privacidad y de anonimato que es intrínseca a estos derechos, y que solo debe ser levantada mediante acciones de origen judicial, proporcionales y necesarias, y nunca de carácter masivo. Como lo enfatizó el Alto Comisionado de las Naciones Unidas para los Derechos Humanos:

> *"**El uso de la tecnología de reconocimiento facial entraña importantes riesgos para el disfrute de los derechos humanos, en particular el***

12Comité de Derechos Humanos. (2019). Observación general núm. 37, Artículo 21: derecho de reunión pacífica. Proyecto revisado del relator, Sr. Christof Heyns. Naciones Unidas.

> ***derecho de reunión pacífica**. A pesar de que en los últimos años esta tecnología ha experimentado avances considerables en cuanto a su precisión, lo cierto es que sigue siendo propensa a cometer errores. Así, por ejemplo, una imagen puede ser considerada erróneamente como una coincidencia (conocida como "falso positivo") y puede acarrear consecuencias importantes para los derechos de una persona, como cuando una persona es señalada erróneamente como sospechosa de cometer un delito, ya que puede ser detenida y encausada. Incluso cuando la tecnología de reconocimiento facial se utiliza con un gran número de personas, sus tasas de error más bajas pueden suponer la señalización inexacta de cientos de personas"*[13].

Las medidas de vigilancia de carácter masivo, y en especial aquellas que hacen uso de tecnologías de reconocimiento facial, constituyen formas desproporcionadas de vigilancia, en especial en ausencia de mecanismos de transparencia y rendición de cuentas que permitan a la ciudadanía ejercer control sobre la información recabada:

> "*(...) La tecnología de reconocimiento facial que se emplea en los grandes actos culturales, las competiciones deportivas importantes, los festivales de música y las reuniones políticas también suscita inquietudes acerca de su proporcionalidad. (...)* ***Estas formas de identificación y recopilación de datos atentan contra el anonimato de la persona en los espacios públicos y ejercen unos "efectos disuasorios" considerables en la decisión de participar en reuniones públicas"***[14].

La necesaria tutela del derecho de reunión pacífica y de asociación en estos autos es consistente con la declaratoria previa de que nos encontramos en la presente causa frente a derechos individuales homogéneos, que son vulnerados por el solo despliegue del SRFP.

5.2. Libertad de movimiento o circulación

El derecho de libertad de circulación, consagrado en el artículo 22 de la

13 Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Informe "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", A/HRC/44/24, 24 de junio 2020, párrafo 31, disponible en: https://undocs.org/es/A/HRC/44/24

14Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Informe Derechos a la libertad de reunión pacífica y de asociación, 17 de mayo 2019, párrafo 56, disponible en: https://undocs.org/es/A/HRC/41/41.

Convención Americana sobre Derechos Humanos, en el artículo 14 de la Constitución Argentina y en el artículo 12 del Pacto de Derechos Civiles y Políticos, prescribe que toda persona que se halle legalmente en el territorio de un Estado tiene derecho a circular por el mismo y a residir en él con sujeción a las disposiciones legales, indicando que cualquier limitación debe ser indicada por la ley y fundada en razones de interés público. En consecuencia, la libertad de movimiento o circulación es imprescindible para asegurar la vida democrática de las sociedades, y no puede ser desalentada a través de sistemas que generen temor en la población de ocupar los espacios públicos para su asociación o expresión.

El derecho humano a la libertad de movimiento significa no solamente la posibilidad de moverse en el espacio en un sentido físico, sino también, y de manera más fundamental, la libertad de moverse sin tener que dejar rastros continuos y frecuentes de nuestros movimientos para efectos de vigilancia. Ha sido establecido en la doctrina que el hecho de "ser visto sin ver", es decir, ser objeto de vigilancia sin tener la capacidad de controlar la información que es recabada sobre nosotros, puede influir la conducta y las actividades de una persona, llevando a comportamientos sumisos por parte de los ciudadanos, que son incompatibles con el ejercicio de otros derechos fundamentales.

Las tecnologías biométricas además capacitan a quien ejerce la vigilancia a ejercer conductas más sofisticadas, como hacer seguimiento de la ruta de una persona o de un vehículo en escenarios complejos, o identificar a las personas que siguen una determinada ruta, o establecer patrones de comportamiento a largo plazo. Al tiempo que estas técnicas pueden ser utilizadas con propósitos legítimos, como encontrar personas desaparecidas, su uso no diferenciado puede acarrear efectos negativos para las libertades ciudadanas que no necesariamente es proporcional al fin buscado. En este sentido, la Corte Interamericana de Derechos Humanos ha establecido que :

> *"cuando una política general o medida tiene un efecto desproporcionado perjudicial en un grupo particular puede ser considerada discriminatoria aún si no fue dirigida específicamente a ese grupo"*[15].

Así, tal como ha declarado el Comité de Derechos Humanos de Naciones Unidas

15Caso Nadege Dorzema y otros vs. República Dominicana. 24 de octubre de 2012.

en la Observación General N° 27 al Pacto Internacional sobre Derechos Civiles y Políticos[16], las restricciones a la libertad de circulación no solo deben ser utilizadas para conseguir fines permisibles, sino que deben ser necesarias para protegerlos:

> *"Las medidas restrictivas deben ajustarse al principio de proporcionalidad; deben ser adecuadas para desempeñar su función protectora; deben ser el instrumento menos perturbador de los que permitan conseguir el resultado deseado, y deben guardar proporción con el interés que debe protegerse"*[17].

De lo anterior se concluye que, al verse potencialmente vigilado e identificado mediante cámaras con tecnología biométrica, el ciudadano común alterará su comportamiento y ajustará sus actividades en respuesta a esta vigilancia, lo que constituye una intromisión impermisible e inaceptable en sus libertades fundamentales de movimiento, reunión y de expresión.

La vigilancia estatal permanente mina la voluntad de los individuos de organizarse, asociarse, participar políticamente en la sociedad y expresarse libremente sin temor a represalias, lo que a su vez representa un costo demasiado elevado para la vida democrática de una nación. Más aún, si los ciudadanos no están debidamente informados del alcance, el propósito y los mecanismos de operación de estos sistemas, será imposible establecer los mecanismos de confianza y de fiscalización democrática, necesarios para que el efecto de enfriamiento se vea –al menos– controlado. En contextos donde preexiste una desconfianza por parte de los ciudadanos hacia sus fuerzas policiales, este efecto se verá sin duda agravado[18].

Por ende, la implementación de sistemas tecnológicos de vigilancia masiva -en especial aquellos que utilizan tecnologías de reconocimiento facial- afecta de manera grave e injustificable los derechos a la privacidad, a la libertad de expresión, al libre tránsito y a la libre asociación y reunión pacífica, al no cumplir con los requisitos mínimos de legitimidad, necesidad y proporcionalidad

16 Comité de Derechos Humanos. Libertad de circulación (art. 12):. 02/11/99. CCPR/C/21/Rev. 1/Add. 9, CCPR Observación General 27.(General Comments). Organización de Naciones Unidas; 1999 feb. Recuperado: https://www.acnur.org/fileadmin/Documentos/BDL/2001/1400.pdf

17 Comité de Derechos Humanos. Libertad de circulación (art. 12):. 02/11/99. CCPR/C/21/Rev. 1/Add. 9, CCPR Observación General 27 (General Comments). Organización de Naciones Unidas; 1999 feb. Recuperado: https://www.acnur.org/fileadmin/Documentos/BDL/2001/1400.pdf

18 Goold, B. J. (2010). *CCTV and Human Rights*. https://papers.ssrn.com/abstract=1875060

tal como se encuentran desarrollados en el marco interamericano de los derechos humanos. Asimismo, la potencial implementación de cualquier tipo de tecnología de vigilancia que esté orientada a cumplir con fines de seguridad pública debe contemplar, desde su diseño, los mecanismos necesarios de transparencia que posibiliten a la ciudadanía ejercer el control de su uso en cuanto respecta a las afectaciones contra sus derechos fundamentales[19].

5.3. Privacidad, intimidad y protección de datos personales

Los derechos de privacidad, intimidad y protección de datos personales, se encuentran amparados a partir de la protección ofrecida a la vida privada en el artículo 11 de la Convención Americana sobre Derechos Humanos, el artículo 17 del Pacto de Derechos Civiles y Políticos, y del artículo 18 de la Constitución Argentina que concede protección a la inviolabilidad del hogar y de las comunicaciones, así como la interpretación progresiva de los mismos emanada del artículo 33 de la Constitución Argentina. Por su parte, el artículo 12 de la Constitución de la Ciudad Autónoma de Buenos Aires garantiza la privacidad, intimidad y confidencialidad como parte inviolable de la dignidad humana.

La tecnología de vigilancia mediante reconocimiento facial en el espacio público opera mediante la detección de individuos para su identificación, y es por tanto necesariamente una tecnología intrusiva e invasiva: consiste en el procesamiento de información biométrica (las características físicas de las personas) a distancia. Aunque la presencia de cámaras fijas de videovigilancia en el espacio público es una realidad previa, la presencia de tecnología de reconocimiento facial, dada su intrusividad, altera el equilibrio de expectativas de riesgo de las personas sobre el uso de su información personal y sobre la afectación de su privacidad.

Las cámaras de identificación biométrica constituyen un avance significativo en las tecnologías digitales. El riesgo de afectación a la privacidad fue relevado por la Asamblea General de las Naciones Unidas en la Resolución 86/167, “El derecho a la privacidad en la era digital” de 2013 y posteriores resoluciones sobre la misma materia, reconociendo que el

19Becker, S., Lara, J .C., & Canales, M. P. (2018). *La construcción de estándares legales para la vigilancia en América Latina*. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-I.pdf

> *"desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones y, al mismo tiempo, incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad, establecido en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, y que, por lo tanto, esta cuestión suscita cada vez más preocupación"*[20].

Si bien la expectativa de privacidad en los espacios públicos no es la misma que en los espacios privados, es necesario hacer énfasis en que el derecho a la privacidad no desaparece en el momento en que cruzamos el umbral de nuestras casas. La mayoría de las personas espera un cierto grado de anonimato y privacidad al llevar a cabo acciones en el espacio público, y la exposición constante al escrutinio de las cámaras de vigilancia despoja al ciudadano de esta privacidad de un modo que es mucho más intenso y constante que la mirada pública, y que está intrínsecamente ligado al poder del Estado[21].

En este sentido, como señaló quien fuera el Supervisor Europeo de Protección de Datos, Giovanni Buttarelli,

> *"**ser vigilado cambia la manera en que nos comportamos**. De hecho, cuando somo vigilados, muchos de nosotros podríamos censurar nuestro discurso y nuestro comportamiento. Éste es ciertamente el caso con la vigilancia continua o extendida. **Saber que cada movimiento y cada gesto es monitoreado por una cámara puede tener un impacto psicológico y cambiar el comportamiento**. Esto constituye una interferencia en nuestra privacidad"*[22].

20Asamblea General de las Naciones Unidas. 20 de noviembre de 2013. El derecho a la privacidad en la era digital. A/RES/68/167. Recuperado: https://undocs.org/pdf?symbol=es/A/RES/68/167

21 Goold BJ. CCTV and Human Rights. 2010: https://papers.ssrn.com/abstract=1875060

22 Buttarelli G. Welcome address: Fundamental rights at stake. EDPS Workshop on Video-surveillance within Community institutions and bodies, 2009, Brussels, https://edps.europa.eu/sites/edp/files/publication/09-09-30_videosurveillance_welcome_address_en.pdf

Por otra parte, el reconocimiento facial automatizado constituye un despliegue tecnológico que altera gravemente la expectativa de control sobre la información personal. La utilización de este tipo de tecnologías implica la recolección masiva de datos personales de carácter sensible, como son los datos vinculados al cuerpo que se recaban, utilizan y procesan por medio de las tecnologías biométricas. Las personas que transitan por espacios así vigilados no pueden ejercer oposición a la captura y análisis de su rostro.

> "*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 seguir con sus vidas 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, el Alto Comisionado acoge con satisfacción los recientes esfuerzos para limitar o prohibir el uso de tecnologías de reconocimiento biométrico en tiempo real"*[23].

La captación de este tipo de datos debería, por ende, requerir de un modelo de consentimiento más estricto que aquel que se requiere para la recolección de otros datos personales, y bajo ningún escenario debería llevarse a cabo de manera pasiva e implícita, o ser obligatoria por defecto, como es el caso de la recolección de datos biométricos llevada a cabo por cámaras de vigilancia en espacios públicos. No es aceptable que una recolección de esa manera ocurra de manera masiva e indiscriminada potencialmente sobre todas las personas, como es el caso de las cámaras de videovigilancia en el espacio público.

En la resolución sobre "El derecho a la privacidad en la era digital" de 2017, el Consejo de Derechos Humanos de las Naciones Unidas reconoce que

23 United Nations High Commissioner for Human Rights. The right to privacy in the digital age report. A/HRC/48/31, 13 de septiembre de 2021.P. 27. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx

> *"**la vigilancia** y/o la interceptación ilegales o arbitrarias de las comunicaciones, **así como la recopilación ilegal o arbitraria de datos personales, al constituir actos de intrusión grave, violan el derecho a la privacidad y pueden interferir con otros derechos humanos**, incluido el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, y el derecho a la libertad de reunión y asociación pacíficas, y ser contrarios a los preceptos de una sociedad democrática, en particular cuando se llevan a cabo extraterritorialmente o a gran escala"*[24] .

Esa recopilación de datos, en consecuencia, constituye una afectación directa sobre la intimidad, que conlleva la imposibilidad de pleno ejercicio de los demás derechos. Como indica Buttarelli, es necesario analizar caso por caso si los mecanismos de control y vigilancia causan un daño desproporcionado a las libertades individuales, en comparación con el potencial beneficio que pueden perseguir. Desde este punto de vista, el uso de mecanismos de vigilancia debe hacerse bajo un criterio selectivo, puesto que el público general no debería sufrir las limitaciones excesivas causadas por la necesidad de evitar el mal comportamiento de una minoría de personas[25].

Según este criterio, de acuerdo con los requisitos propios del Sistema Interamericano, toda medida de intrusión al derecho a la privacidad debe tener como requisito previo la existencia de una orden judicial que indique de manera clara y precisa el alcance y duración de la medida, los hechos que la justifican, los organismos competentes para llevarlas a cabo y sus facultades específicas, en referencia a individuos específicos. Estos requisitos cumplen con un doble objetivo: por un lado, permitir al ciudadano el conocimiento preciso y delimitado de la restricción a sus derechos, y por otro, garantizar la posibilidad del ejercicio de un control efectivo sobre las medidas, control que sería imposible llevar a cabo bajo criterios de opacidad o secreto[26].

La recolección masiva de datos personales sensibles que permite el reconocimiento facial a distancia conlleva adicionalmente un riesgo importante

24 Naciones Unidas, resolución del Consejo de Derechos Humanos, 'El derecho a la privacidad en la era digital', A/HRC/34/L.7/Rev.1, Naciones Unidas, Nueva York, 2017, preámbulo.
25 Buttarelli G. Welcome address: Fundamental rights at stake. Op. cit.
26ONU, OEA. Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión. 2013 [citado 18 de febrero de 2020]. Recuperado: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

de que dicha información si no resulta custodiada con las medidas de seguridad adecuada genere en manos de terceros actores maliciosos una pérdida completa del control de su propia identidad por los titulares de tales datos. Un sistema como el SRFP, implementado sin evaluación previa de sus impactos de privacidad y sin mecanismos de seguridad claros y transparentes para la ciudadanía expone a los millones de habitantes de la Ciudad de Buenos Aires a un riesgo exponencial de pérdida de control de su identidad que no se justifica en forma proporcional con cualquier fin de interés público perseguido por dicho sistema.

Por último, el potencial de las tecnologías de reconocimiento facial para perfilar y perseguir a periodistas, defensores de derechos humanos y disidentes políticos, constituye un riesgo adicional sobre actividades ya peligrosas, que a su vez implica el deber de los Estados de adoptar salvaguardas domésticas que protejan a los individuos de la vigilancia indebida[27]. Esto implica que, además de los resguardos institucionales para la implementación de estas tecnologías y su uso bajo criterios de legalidad, necesidad y proporcionalidad, la sociedad civil debe tener la capacidad de supervisar la adopción y utilización de tales tecnologías, así como de ejercer mecanismos de control y rendición de cuentas que garanticen que se cumplan las salvaguardas necesarias.

5.4. Libertad de expresión

La libertad de expresión se encuentra consagrada en el artículo 13 de la Convención Americana sobre Derechos Humanos, protección que incluye el que dicha libertad no sea restringida por vías o medios indirectos. En el mismo sentido, el artículo 19 del Pacto de Derechos Civiles y Políticos, y los artículos 14 de la Constitución Argentina y 32 de la Constitución de la Ciudad Autónoma de Buenos Aires protegen la libre expresión.

La implementación de sistemas de vigilancia erosiona la privacidad de las personas y con ello afecta a otros derechos humanos. Tal como ha señalado la CIDH, la recopilación de datos personales puede afectar la libertad de expresión, y los sistemas de televigilancia, en especial aquellos que utilizan

27 Moratorium call on surveillance technology to end “free-for-all” abuses: UN expert. En: UN News [Internet]. 25 de junio de 2019. Recuperado: https://news.un.org/en/story/2019/06/1041231

tecnologías biométricas, constituyen una amenaza para el sistema democrático[28].

Toda restricción a la libertad de expresión debe cumplir con el requisito de ser legítima, necesaria y proporcional. En lo que respecta a la necesidad de la medida, tal como indica la Declaración Conjunta sobre la Libertad de Expresión y las respuestas a las situaciones en conflicto, la vigilancia indiscriminada o masiva es siempre desproporcionada en cuanto por definición abarca a una población extensa e indeterminada:

> *"la vigilancia debería llevarse a cabo solo de forma limitada y selectiva y de una manera que represente un equilibrio adecuado entre el orden público y las necesidades de seguridad, por un lado, y los derechos a la libertad de expresión y a la privacidad, por el otro.* ***La vigilancia indiscriminada o masiva, es inherentemente desproporcionada y constituye una violación de los derechos de privacidad y libertad de expresión****"*[29].

Respecto a las cámaras de vigilancia con reconocimiento facial en particular, el Consejo de Derechos Humanos de la ONU ha señalado que su utilización arbitraria constituye un acto de intrusión grave en la privacidad, que puede "*interferir con el derecho a la libertad de expresión, de reunión y asociación pacífica y ser contrarios a los preceptos de una sociedad democrática, en particular cuando se llevan a cabo a gran escala"*[30].

Este tipo de vigilancia, genera lo que se ha denominado un "efecto de enfriamiento" sobre la libertad de expresión, esto es, el efecto de desincentivar o disuadir a las personas de expresarse libremente, en especial de expresar opiniones que pueden resultar contrarias al statu quo, incómodas o impopulares. En tal sentido, tanto la entonces Relatora Especial para la

28 Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Estándares para una Internet Libre, Abierta e Incluyente. OEA/Ser.L/V/II CIDH/RELE/ INF.17/17.
http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf

29 Comisión Interamericana de Derechos Humanos. Declaración conjunta sobre la libertad de expresión y las respuestas a situaciones en conflicto. Organización de Estados Americanos; 4 de mayo de 2015. http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=987&lID=2

30 Consejo de Derechos Humanos, Asamblea General de Naciones Unidas. El derecho a la privacidad en la era digital. A/HRC/28/L.27. Organización de las Naciones Unidas; 24 de marzo de 2015. https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf

Libertad de Expresión de la CIDH y el Relator Especial de la ONU para la Protección y Promoción del Derecho a la Libertad de Opinión y Expresión declararon, en visita a México, que:

> *"la tecnología de vigilancia tiene implicaciones profundas para ejercer la libertad de expresión, que perjudican la capacidad de los individuos para compartir o recibir información y establecer contacto con activistas y otros. Crea incentivos para la autocensura y directamente perjudica la capacidad de los periodistas y defensores de derechos humanos para realizar investigaciones y construir y mantener relaciones con fuentes de información"*[31].

Tal efecto no se limita a formas limitadas o selectivas de vigilancia, sino sobre cualquier acto expresivo o informativo realizado bajo la observación de tecnología de vigilancia con la capacidad de identificar a individuos en el espacio público. Esa identificación automatizada niega ilegítimamente la capacidad de participar anónimamente en la esfera pública. Según el ex Relator Especial sobre Libertad de Expresión de Naciones Unidas, Frank La Rue, las interferencias ilícitas al anonimato crean límites indebidos a la libertad de expresión:

> *"La interferencia indebida con la privacidad de los individuos puede limitar directa e indirectamente el libre desarrollo e intercambio de ideas. Las restricciones al anonimato en las comunicaciones, por ejemplo, tienen un evidente efecto de enfriamiento en las víctimas de todas las formas de violencia y abuso, quienes pueden ser reacias a reportar por miedo a la doble victimización"*[32].

De manera análoga a lo que ocurre con la vigilancia de comunicaciones, la vulneración de la capacidad de desenvolverse de manera anónima en la vida civil, incluido el ejercicio del derecho a la libertad de expresión en el espacio público. Es decir, puesto que el propósito directo de la tecnología de reconocimiento facial es vincular a personas en el espacio público con factores

31 ACNUDH. Observaciones preliminares del Relator Especial de la ONU sobre la libertad de expresión y el Relator Especial sobre libertad de expresión de la CIDH después de su visita conjunta en México, 27 de noviembre – 4 de diciembre 2017.

32 Human Rights Council. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. https://www.ohchr.org/ Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

identificadores en poder del vigilante, la imposibilidad de ejercicio del anonimato sin esfuerzos adicionales redundará en el comportamiento autolimitado de quien se siente bajo observación.

Más gravemente, el efecto de enfriamiento que la vigilancia tiene sobre la población afecta de manera más aguda y específica a las minorías, lo que trae como consecuencia que –en particular en cuanto se refiere a las víctimas de violencia y abuso– puede significar un obstáculo importante en sus posibilidades para acceder a la justicia, afectando así de manera más amplia y más profunda la protección y el ejercicio efectivo de sus derechos humanos.

5.5. No discriminación

El derecho a la igualdad o a no ser discriminado se encuentra consagrado en los artículos 1 y 24 de la Convención Americana sobre Derechos Humanos. El Pacto Internacional de Derechos Civiles y Políticos además de reconocer el derecho general a la no discriminación en su artículo 26, determina el derecho a las medidas de protección de los niños sin discriminación alguna,en su artículo 24. En el mismo sentido, los artículos 16 y 37 de la Constitución Argentina y artículo 11 de la Constitución de la Ciudad Autónoma de Buenos Aires.

El reconocimiento facial ha sido ampliamente cuestionado por las altas tasas de falsos positivos que arroja. Este problema aumenta exponencialmente cuando las personas que están siendo vigiladas pertenecen a grupos históricamente vulnerados como mujeres, personas de piel oscura o personas trans. La implementación de sistemas de reconocimiento facial conlleva la reproducción técnica de los sesgos de exclusión social y, cuando son utilizados con fines de vigilancia, amenaza el derecho a la dignidad, al debido proceso y la presunción de inocencia.

> *"Además,* ***la tecnología de reconocimiento facial puede perpetuar y amplificar la discriminación, incluso contra los afrodescendientes y otras minorías, las mujeres o las personas con discapacidad, porque puede utilizarse para el perfilado de personas sobre la base de su etnia, raza, origen nacional, género y otras características****. Esta tecnología también puede dar lugar a una discriminación involuntaria, ya que*

su precisión depende de factores como el color de la piel o el género; de hecho, ***la experiencia ha demostrado que las tasas de precisión en el caso del reconocimiento de personas de piel oscura y mujeres son menores****"*[33].

Investigaciones realizadas particularmente en los países del norte global donde estas tecnologías han sido desarrolladas inicialmente, muestran su capacidad, para reproducir y exaltar los sesgos que potencialmente articulan mecanismos de discriminación arbitrarios en función de criterios como el sexo, la edad o el color de la piel[34].

Al evaluar la aplicación de tales tecnologías por parte de los Estados, no solo es preocupante la posible aparición de esas formas de discriminación, sino también la debilidad institucional del Estado en generar mecanismos de identificación y control de los impactos negativos de tales discriminaciones. Esto se traduce en ceguera institucional al considerar, por ejemplo, grupos marginados y vulnerables (por edad, ubicación geográfica, origen étnico, género, entre otros) que son "invisibles" cuando el Estado actúa y diseña sus políticas.

Debido al nivel actual de errores y fallas y el impacto en los no caucásicos en términos de libertades civiles y derechos humanos, las propias empresas de desarrollo tecnológico han tomado la iniciativa en no ofrecer software de reconocimiento facial. Por ejemplo empresas como Amazon[35], Microsoft[36] y IBM[37] entendieron expresamente que deberían detener su oferta por algún

33 Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Informe "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", A/HRC/44/24, 24 de junio 2020, párrafo 32, disponible en: https://undocs.org/es/A/HRC/44/24

34 Sidhu, D. S. (2011). *The Chilling Effect of Government Surveillance Programs on the Use of the Internet By Muslim-Americans*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002145

35 El País. "Amazon suspende indefinidamente la venta de su tecnología de reconocimiento facial a la policía". https://elpais.com/tecnologia/2021-05-21/amazon-suspende-indefinidamente-la-venta-de-su-tecnologia-de-reconocimiento-facial-a-la-policia.html

36 The Washington Post. "Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM". https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/

37 El País, "IBM abandona la tecnología de reconocimiento facial por las dudas éticas

tiempo. En una declaración contundente al Congreso de los EE. UU., la empresa multinacional estadounidense de tecnología y consultoría IBM, declaraba:

> *"IBM se opone firmemente y no tolerará el uso de ninguna tecnología,* ***incluida la tecnología de reconocimiento facial ofrecida por otros proveedores, para la vigilancia masiva, la determinación de perfiles raciales, las violaciones de los derechos humanos y las libertades básicas, o cualquier propósito que no sea coherente con nuestros valores y principios de Confianza y Transparencia****. Creemos que ahora es el momento de iniciar un diálogo nacional sobre si los organismos nacionales encargados de hacer cumplir la ley deben emplear la tecnología de reconocimiento facial y cómo".*[38]

El proyecto "The Gender Shades", realizado por las investigadoras Joy Buolamwini y Timnit Gebru, evalúa la precisión de los productos de clasificación de género impulsados por sistemas de reconocimiento facial que utilizan inteligencia artificial (IA), centrándose en las clasificaciones de género como ejemplo motivador para mostrar la necesidad de una mayor transparencia en el rendimiento de cualquier producto y servicio de IA que se centre en sujetos humanos. El sesgo en este contexto se define como diferencias prácticas en las tasas de error de clasificación de género entre grupos. El estudio muestra que existen diferencias notables en las tasas de error entre los diferentes grupos. Todas las empresas obtienen mejores resultados en sujetos más claros en su conjunto que en sujetos más oscuros en general, con una diferencia del 11,8 % al 19,2 % en las tasas de error. Según este estudio, por ejemplo, IBM tenía la mayor brecha en precisión, con una diferencia del 34,4 % en la tasa de error entre hombres más claros y mujeres más oscuras. En casos aún más expresivos, el análisis de errores revela que el 93,6% de los rostros mal identificados por Microsoft eran los de sujetos más oscuros. Sin embargo, la tasa de error máxima para los machos de piel más clara es del 0,8 %[39].

sobre su uso". https://elpais.com/tecnologia/2020-06-09/ibm-abandona-la-tecnologia-de-reconocimiento-facial-por-las-dudas-eticas-sobre-su-utilizacion.html

38 IBM. "IBM CEO's Letter to Congress on Racial Justice Reform". 8 de junio de 2020. https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/.

39 Buolamwini J.; Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research 81:1–15, 2018. Recuperado: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

En 2019, el National Institute of Standards and Technology (NIST), un organismo oficial de los Estados Unidos, publicó un estudio sobre los sesgos demográficos de la tecnología de reconocimiento facial disponible a la fecha. Los investigadores encontraron que los algoritmos de reconocimiento facial funcionan peor al examinar los rostros de mujeres, personas de color, ancianos y niños, lo que genera serias preocupaciones sobre el uso policial de la tecnología en los Estados Unidos y el mundo, y subraya la necesidad de presionar pausa en el uso gubernamental de la tecnología. Este estudio, único en su tipo en el mundo, abarca los resultados de pruebas a 189 algoritmos de 99 proveedores distintos. Las diferencias en el nivel de precisión del reconocimiento facial no resultan menores, si no que por el contrario son preocupantes dadas las tasas de falsos positivos, o la frecuencia con la que una cara se identificó erróneamente como otra persona. La mayoría de los algoritmos encuentran entre 10 y 100 veces más coincidencias falsas para las mujeres negras que para los hombres blancos, según el estudio. Asimismo, las mujeres blancas tampoco se encuentran libres de errores de identificación significativos, ya que las tasas de coincidencia falsa de la mayoría de los algoritmos es entre 2 y 10 veces más altas que las de los hombres blancos. Las disparidades son menores para las tasas de falsos negativos, pero aún muestran sesgos contra las caras no “europeas”[40].

En julio de 2019, un informe independiente sobre el ensayo de tecnología de reconocimiento facial en vivo (LFR) del Servicio de Policía Metropolitana de Londres, escrito por el profesor Pete Fussey y el Dr. Daragh Murray de la Universidad de Essex[41], llegó a la conclusión de que sería "muy posible" que el uso de LFR hasta la fecha se considerara ilegal si se impugnara en un tribunal, ya que existen graves delitos contra los derechos humanos. También han documentado deficiencias operativas significativas en los ensayos que podrían afectar la viabilidad de cualquier uso futuro de la tecnología LFR. El estudio demostró que el sistema hizo 42 coincidencias, pero en solo ocho de esas

40 Patrick Grother, Mei Ngan, Kayee Hanaoka. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, National Institute of Standards and Technology, U.S. Department of Commerce, December 2019. Disponible en: https://doi.org/10.6028/NIST.IR.8280

41 Fussey, P. Murray, D. Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology. The Human Rights, Big Data and Technology Project. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

coincidencias, los autores del informe pueden decir con absoluta confianza que la tecnología lo hizo bien.

Sin embargo, es necesario señalar que aunque pudiera existir una tecnología más precisa, ello no resolverá el impacto desproporcionado que las altas tasas de identificación mal realizada de las personas más vulnerables (ya sea por razones de género o raciales) tiene en "potenciar un sistema de aplicación de la ley con una larga historia de vigilancia racista y antiactivista y puede ampliar las desigualdades preexistentes"[42]. Es decir, aceptar la tasa de sesgo de un sistema de reconocimiento facial como el SRFP constituye una decisión política de afectar a priori en forma desproporcionada la garantía de igualdad frente a la ley de grupos tradicionalmente discriminados y vulnerables, como pueblos originarios, mujeres, niños, adultos mayores y personas trans.

En relación al derecho de los niños a no ser discriminados, la materia ha sido objeto específico de críticas en el despliegue del SRFP. Como destacó el Relator Especial de las Naciones Unidas sobre el derecho a la privacidad, Señor Joseph Canatacci en el texto ya transcrito en esta pieza, existen problemas de discriminación también relacionados con los niños[43]. Un estudio publicado por Human Rights Watch ("HRW"), concluyó que la base de datos que alimenta el sistema de reconocimiento facial viola los derechos de los niños en los procesos penales e incluye errores importantes[44].

Según el estudio de HRW, al menos 166 menores han aparecido en la lista de la CONARC entre mayo de 2017 y mayo de 2020, incluyendo niños sospechosos de cometer delitos menores, y que el delito más común del cual se acusa a menores de edad es el de robo, en el 37,5% de los casos. Existe, por tanto, una

42 NAJIBI, Alex. Racial Discrimination in Face Recognition Technology.Harvard University Blog, Science Policy and Social Justice Edition.October 24 2020. Recuperado: <http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>

43 Canatacci, Joseph. 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. https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=S

44 Human Rights Watch. Carta al Lic. Horacio Rodríguez Larreta sobre el Sistema de Reconocimiento Facial de Prófugos y derechos de niñas y niños (Washington D.C., 9 de octubre de 2020). Recuperado: https://www.hrw.org/es/news/2020/10/09/carta-al-lic-horacio-rodriguez-larreta-sobre-el-sistema-de-reconocimiento-facial-de#_ftn3

violación al artículo 24, del Pacto Internacional de Derechos Civiles y Políticos.

6. Materialidad del daño y riesgos de seguridad

El sistema de reconocimiento facial permite una vigilancia masiva permanente de la población, violando claramente los derechos humanos, como se discutió en la sección anterior. Sin embargo, es importante destacar los peligros reales e inmediatos a los que están expuestos los ciudadanos.

En el caso específico de Buenos Aires y el sistema instalado, ya existen casos de detenciones arbitrarias e ilegales, constantes errores en el sistema e incluso la presencia de niños, niñas y adolescentes en listas criminales, sin respeto al debido proceso legal necesario para evitar la discriminación y para respetar todos los derechos humanos. Estos problemas son consistentes con errores, detenciones ilegales y discriminaciones por reconocimiento facial que también se han registrado en varias partes del mundo, como Nueva York, Río de Janeiro, Salvador, Londres, Gales, entre otras.

Entonces no es de extrañar que desde la academia se ha denunciado que este tipo de tecnología se ha convertido en la más peligrosa herramienta de vigilancia jamás inventada, gracias a los avances en IA, la proliferación de la fotografía, la disminución de los costos de almacenamiento de grandes conjuntos de datos en la nube y el acceso barato a las tecnologías de reconocimiento facial:

> *“**Creemos que la tecnología de reconocimiento facial es el mecanismo de vigilancia más peligroso jamás inventado**. Es la pieza que falta en una infraestructura de vigilancia ya peligrosa, construida porque esa infraestructura beneficia tanto al gobierno como al sector privado. **Y cuando las tecnologías se vuelven tan peligrosas y la relación daño-beneficio se vuelve tan desequilibrada, vale la pena considerar las prohibiciones categóricas.** La ley ya prohíbe ciertos tipos de tecnologías digitales peligrosas, como el software espía. La tecnología de reconocimiento facial es mucho más peligrosa. (...) **La vigilancia realizada con sistemas de reconocimiento facial es intrínsecamente opresiva**.*

La mera existencia de sistemas de reconocimiento facial, que a menudo son invisibles, perjudica las libertades civiles, porque las personas actuarán de manera diferente si sospechan que están siendo vigiladas. Incluso la legislación que promete procedimientos de protección estrictos no evitará que el frío obstaculice oportunidades cruciales para el florecimiento humano al frenar la conducta expresiva y religiosa"[45].

Sumado a la falta de rendición efectiva de los cuentas de los sistemas de IA, Selinger y Hartzog enfatizan muy claramente que:

"La tecnología de reconocimiento facial también permite una serie de otros abusos y actividades corrosivas [...]:

- *Impacto desproporcionado en las personas de color y otros poblaciones minoritarias y vulnerables.*
- *Daños al debido proceso, que pueden incluir el cambio de ideal de 'presunta inocencia' a 'personas que han todavía no ha sido declarado culpable de ningún delito'.*
- *Facilitar el acoso y la violencia.*
- *Negación de derechos y oportunidades fundamentales, tales como protección contra el 'seguimiento arbitrario del gobierno de los propios movimientos, hábitos, relaciones, intereses, y pensamientos'.*
- *La sofocante moderación del implacable, perfecto cumplimiento de la ley.*
- *La eliminación normalizada de la opacidad práctica.*
- *Epidermización digital y ciencia basura aplicada (por ejemplo, frenología digital).*
- *La amplificación del capitalismo de vigilancia.*
- *Vulnerabilidades de seguridad".*[46]

La falta de información más básica por parte del Estado sobre el sistema de reconocimiento facial, sumado a los problemas relacionados con las violaciones a la libertad de expresión, al derecho de reunión, al respeto a los derechos de los niños, y también con las medidas discriminatorias, debidas a cuestiones

45 Selinger, Evan; Hartzog, Woodrow. Facial Recognition Is the Perfect Tool for Oppression.Medium. https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

46 Selinger, E.; Hartzog, W., The Inconsentability of Facial Surveillance (March 19, 2020). 66 Loyola Law Review 101 (2019). Recuperado: https://ssrn.com/abstract=3557508

estructurales intrínsecas de la sociedad y exacerbadas por falsos positivos y fallas técnicas que perjudican aún más a personas vulnerables, llevan a pensar que el peligro es real e inminente. Como señaló la Alta Comisionada de las Naciones Unidas para los Derechos Humanos en su ultimo informe "el riesgo de discriminación relacionado con las decisiones basadas en la inteligencia artificial es demasiado real"[47].

A todo lo anterior se suman los riesgos derivados de potenciales fallas o carencias en las medidas de seguridad digital, destinadas a resguardar la disponibilidad, integridad y confidencialidad de los datos personales recogidos a través del SRFP. En virtud de lo dispuesto en artículo 9 de la LPDP, *"El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado"*. A la fecha, como consta en los autos de acceso a la información pública pedidos traer a la vista por la actora en esta causa, el GCBA ha fallado en proporcionar información sobre las características de las medidas de seguridad de la información adoptadas en el despliegue del SRFP.

¿Cuáles son los puntos de vulnerabilidad a los cuáles puede estar expuesto un sistema de reconocimiento facial? La seguridad del reconocimiento facial es un proceso complejo que involucra el análisis de diferentes áreas de seguridad. Por una parte, debe garantizarse la seguridad de la infraestructura en que el sistema funciona, esto es, el hardware, la plataforma, las aplicaciones y los marcos. Luego, debe garantizarse la seguridad del modelo algorítmico que realiza la comparación de rostros, que puede sufrir ataques de adversarios externos, "como envenenamientos" de set de datos (cambios o alteración que alteran su nivel de efectividad), puertas traseras que permitan la captura de los

47 ACNUDH. Informe "The right to privacy in the digital age report". A/HRC/48/3, 13 de septiembre de 2021. Párrafo 57. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx

datos recogidos, entre otros[48]. Se requiere demostrar que existen medidas técnico organizacionales suficientes para garantizar la seguridad de ambas capas.

A este respecto la Relatora Especial de las Naciones Unidas para la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo ha recomendado lo siguiente:

> *"Los Estados deben asegurarse de que los datos biométricos se incluyan en el ámbito de las leyes de protección de datos y de que la protección pertinente no se restrinja indebidamente incluso cuando dichos datos se recopilen, conserven, procesen o compartan en un contexto de seguridad nacional"*[49].

Más adelante, agrega:

> *"Las decisiones de retener datos biométricos también deben considerar cuestiones relacionadas con la seguridad de los datos y el riesgo de que los datos biométricos se vean comprometidos. Ciertas modalidades de almacenamiento, como la creación de bases de datos centralizadas, plantean un riesgo mayor que el almacenamiento localizado de dichos datos. A este respecto, se debe prestar la debida atención a las posibles consecuencias graves y, en ocasiones, irreversibles que se deriven del uso indebido o el compromiso de los datos biométricos. Además de los riesgos relacionados con la seguridad, los períodos de retención prolongados también aumentan el riesgo de "desviación de misión" y puede dar lugar a un uso más allá del propósito para el que se recopilaron los datos.*
>
> *"Recomendaciones:*
>
> - *El cumplimiento de los derechos humanos de las medidas que involucran datos biométricos debe ser debidamente evaluado en cada*

48 Ver Yigit Alparslan, Ken Alparslan, Jeremy Keim-Shenk, Shweta Khade, Rachel Greenstadt.
"Adversarial Attacks on Convolutional Neural Networks in Facial Recognition Domain", Cornell University, disponible en: arXiv:2001.11137v3 [cs.LG]

49 Krisztina Huszti-Orbán y Fionnuala Ní Aoláin. Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?Report prepared under the aegis of the Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Human Rights Center, University of Minesota, 2020, p.17, disponible en: https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf

etapa del uso de los datos.

- *Los datos deben ser desechados de manera segura y apropiada tan pronto como su retención no cumpla con los requisitos de legalidad, necesidad o proporcionalidad. La retención indefinida de datos es incompatible con las obligaciones de los Estados en materia de derechos humanos* "[50].

No es una exigencia de la legislación la creación de sistemas infalibles a brechas de seguridad de la información. No obstante, la implementación de sistemas de recolección y procesamiento de información que, desde su inicio, no han sido formulados en cumplimiento de las expectativas normativas sobre medidas suficientes de seguridad, implica un desconocimiento de las reglas que disponen dichos principios. La utilización de sistemas de reconocimiento facial que recogen y transmiten datos sensibles como hemos visto, se convierte así en fuente de riesgo para los derechos fundamentales de las personas ya que no puede garantizar que el manejo de los datos escape al control del responsable del SRFP, ni tampoco prevé medidas específicas de reclamo o reparación de los datos de los titulares de los datos en caso que se produzca esa pérdida de control y utilización desviada de los datos para otros fines, ya sea por la autoridad o por terceros maliciosos.

Todo lo anterior se exacerba por la naturaleza no voluntaria de la recogida de datos que se produce en un sistema de reconocimiento facial desplegado en la vía pública, sin posibilidad de que la población afectada pueda intervenir a través de su consentimiento.

7. Análisis de legalidad, necesidad y proporcionalidad para la restricción de derechos fundamentales lesionados

Para analizar la legalidad, necesidad y proporcionalidad del acto normativo y el propio sistema de reconocimiento facial, es necesario tener en cuenta cuáles son los elementos y requisitos necesarios para imponer excepciones a los derechos fundamentales. En este sentido, el primer requisito es que esta injerencia del Estado no sea arbitraria o ilegal. Pero hay una importante

50 Ibid. página. 24

diferencia con lo que se considera ilegal porque no necesariamente significa que porque exista una ley aprobada por el Estado no existirá ilegalidad. Este acto normativo en sí mismo debe tener un objetivo específico y proporcional que le brinde legitimidad, y no contener arbitrariedades. Según la Alta Comisionada de Derechos Humanos de las Naciones Unidas recientemente ha afirmado:

> *"El término "ilegal" significa que los Estados pueden interferir con el derecho a la privacidad sólo sobre la base de la ley y de conformidad con esa ley. La propia ley debe cumplir con las disposiciones, propósitos y objetivos del Pacto Internacional de Derechos Civiles y Políticos y* ***debe especificar en detalle las circunstancias precisas en las que dicha injerencia es permisible****. La introducción del concepto de arbitrariedad tiene por objeto garantizar que incluso las injerencias previstas por la ley se ajusten a las disposiciones, fines y objetivos del Pacto y, en todo caso, sean razonables en las circunstancias particulares. En consecuencia, cualquier injerencia en el derecho a la privacidad debe tener un propósito legítimo, ser necesaria para lograr ese propósito legítimo y ser proporcionada.* ***Cualquier restricción también debe ser la opción menos intrusiva disponible y no debe alterar la esencia del derecho a la privacidad"***[51].

Continúa la Alta Comisionada detallando el estándar recién descrito en su reporte, señalando la necesidad de que la implementación de tecnologías que restrinjan la privacidad deben ir acompañadas de un estudio técnico y jurídico que avale cómo ellas resultan apropiadas para los objetivos legítimos propuestos, y no los excedan, o existan medios menos lesivos de alcanzar resultados similares:

> *"(...) En la práctica, eso significa que los Estados deben determinar cuidadosamente si una medida puede lograr un objetivo establecido, cuán importante es ese objetivo y cuáles serán los impactos de la medida. Los Estados también deberían determinar si los enfoques menos invasivos podrían lograr los mismos resultados con la misma eficacia; si es así, se deben tomar esas medidas. El Alto Comisionado ya ha esbozado esas limitaciones y salvaguardias necesarias en el contexto de la vigilancia por parte de los organismos de inteligencia y las fuerzas del orden.* ***Cabe***

51 Op. Cit. Párrafo 8.

> ***señalar que las pruebas de necesidad y proporcionalidad también pueden llevar a la conclusión de que no se deben tomar determinadas medidas.*** *(...) Por ejemplo, antes de decidir desplegar nuevas herramientas de vigilancia basadas en IA, un Estado debe hacer un balance de las capacidades existentes y sus efectos en el disfrute del derecho a la privacidad y otros derechos"*[52].

El Sistema Interamericano de protección de derechos humanos también ha sido activo en reconocer los riesgos de las tecnologías de vigilancia y la necesidad de aplicar los estándares de legalidad, necesidad y proporcionalidad:

> *"En este marco, cabe recordar según lo expresado por la Relatoría Especial para la Libertad de Expresión de la CIDH que: "(l)a protección del derecho a la vida privada implica al menos dos políticas concretas vinculadas al ejercicio del derecho a la libertad de pensamiento y expresión: la protección del discurso anónimo y la protección de los datos personales". También que "los Estados están obligados a prohibir el uso de los datos personales para fines contrarios a los tratados de derechos humanos y a establecer derechos de información, corrección y -de ser necesario y proporcionado- eliminación de datos, así como a crear mecanismos de supervisión efectivos". Respecto a la vigilancia de las comunicaciones cibernéticas la CIDH subraya que "la vigilancia en todas sus modalidades constituye una injerencia en la vida privada". No obstante, "no toda injerencia es per se ilegitima y existen supuestos, excepcionales, que justifican distintos niveles de injerencia de acuerdo con las circunstancias". De este modo, a fin de verificar la legitimidad de cualquier injerencia estatal o no estatal en la vida privada, el sistema interamericano, en consonancia con el universal y el europeo, estableció un test tripartito. Según este test, la medida de vigilancia debe estar sustentada legalmente, en sentido formal y material, ser necesaria y proporcional. Sobre el particular, es importante destacar que la CIDH y su Relatoría Especial para la Libertad de Expresión han indicado que "**las medidas de vigilancia deben ser ordenadas por un juez u órgano jurisdiccional competente, independiente e imparcial y la orden que habilite debe estar debidamente fundada para que la misma sea legítima**"*[53].

52 United Nations High Commissioner for Human Rights. A/HRC/48/31. Op. Cit. Párrafo 39.

53 Comisión interamericana de derechos humanos. Informe "Empresas y Derechos

Difícilmente vemos como las normas impugnadas en esta acción de constitucionalidad y el SRFP en sí mismo podrían satisfacer el estándar recién enunciado, y si hubiera alguna evidencia del análisis aquí delineado el GCBA no ha sido capaz de ponerlo en conocimiento de la ciudadanía para sostener la legitimidad de su decisión.

Como hemos examinado en este apartado, la exigencia de legalidad, necesidad y proporcionalidad en la afectación de derechos humanos por tecnologías de vigilancia masiva como el SRFP analizado en estos autos cuenta con un alto estándar para poder determinar su compatibilidad con las obligaciones del Estado Argentino en la materia, y aún más, pesan en la actualidad serias dudas en los organismos especializados del sistema de protección de derechos humanos de si, siquiera es posible que un sistema de estas características pueda pasar alguna vez el test de evaluación enunciado. Veremos en el próximo apartado que esas recomendaciones se multiplican desde la experiencia internacional, que han formulado prevenciones o tomado acciones específicas en la materia.

8. Recomendaciones de órganos de las Naciones Unidas, Sistema Interamericano de Derechos Humanos y experiencia comparada en materia de regulación de tecnologías de vigilancia

Desde la experiencia de la Unión Europea, en palabras del actual Supervisor Europeo de Protección de Datos, la decisión de adopción de un sistema de reconocimiento facial no resulta una cuestión meramente técnica o de eficacia en un objetivo de política pública, sino que está dotada de una fuerte carga política para una sociedad democrática:

> *"Parece que se está promoviendo el reconocimiento facial como solución a un problema que no existe. Es por eso que varias jurisdicciones de todo el mundo se han movido para imponer una moratoria sobre el uso de la*

Humanos: Estándares Interamericanos", Relatoría Especial sobre Derechos Económicos Sociales Culturales y Ambientales , 2019, párrafo 282: https://www.oas.org/es/cidh/informes/pdfs/EmpresasDDHH.pdf.

tecnología.

"Necesitamos evaluar no solo la tecnología por sus propios méritos, sino también la probable dirección de viaje si continúa utilizándose cada vez más. La siguiente etapa será la presión para adoptar otras formas de objetivación del ser humano, la marcha, las emociones, las ondas cerebrales. Ahora es el momento de que la UE, mientras discute la ética de la IA y la necesidad de regulación, determine si, ***si es que alguna vez, se puede permitir la tecnología de reconocimiento facial en una sociedad democrática.*** *Si la respuesta es afirmativa, solo entonces cambiamos las preguntas sobre cómo y las salvaguardias y la responsabilidad que se deben implementar"*[54].

En el mismo sentido se ha pronunciado Relatora Especial de las Naciones Unidas para la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, haciendo un llamado a una regulación previa compatible con los derechos humanos antes de siquiera considerar su implementación:

"El impacto en los derechos humanos vinculado al uso de herramientas y datos biométricos es enorme. Las consecuencias relacionadas se sienten en una variedad de derechos fundamentales, incluidos, entre otros, los derechos a la vida, la libertad y la seguridad de la persona, el derecho a no ser sometido a tortura, tratos crueles, inhumanos o degradantes, el derecho a un juicio justo, la privacidad y la vida familiar, la libertad de expresión o movimiento, etc. Es la escala de la afectación, junto con la naturaleza universal, interdependiente e interconectada de estos derechos, lo que lleva a efectos múltiples e interrelacionados en una serie de libertades individuales y colectivas que hacen que una regulación compatible con los derechos humanos del uso de herramientas y datos biométricos sea una necesidad imperativa y urgente"[55].

El reconocimiento amplio es que se trata justamente de un estándar alto para determinar su compatibilidad con el respeto de los derechos humanos, como examinamos en el apartado anterior. Dado que hay hipótesis en que no se

54 Wiewiórowski, W. Facial recognition: A solution in search of a problem? 28 de octubre de 2019. https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en

55 Krisztina Huszti-Orbán y Fionnuala Ní Aoláin. Op. Cit. página 14.

avizora posibilidad de cumplimiento de tales estándares, es que en 2019 el entonces Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de la ONU, emitió un llamado para generar la moratoria de exportación, venta, transferencia, uso o prestación de servicios de tecnologías de vigilancia ***"hasta que se establezca un régimen de salvaguardias que respete los derechos humanos"***[56]. El más reciente informe del la Alta Comisionada de Derechos Humanos de Naciones Unidas, ya citado, recoge esa recomendación y la dirige en particular a los sistemas que se alimentan de inteligencia artificial, como es el caso de los de reconocimiento facial, en cuanto sistemas de vigilancia que se han masificado:

> *(...) Cuanto mayor sea el riesgo para los derechos humanos, más estrictos deberían ser los requisitos legales para el uso de la tecnología de IA [inteligencia artificial]. En consecuencia, los sectores en los que hay mucho en juego para las personas, como la aplicación de la ley, la seguridad nacional, la justicia penal, la protección social, el empleo, la atención de la salud, la educación y el sector financiero, deberían tener prioridad. 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"***[57].

Por ello, concluye ampliando sus recomendaciones formuladas el año anterior a los Estados en materia de uso de tecnología de reconocimiento facial en

56 Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión para las Naciones Unidas, Informe "La vigilancia y los derechos humanos", presentado al Consejo de Derechos Humanos, A/HRC/41/35, 28 de mayo 2019, párrafo 66 a), disponible en: https://undocs.org/es/A/HRC/41/35

57 United Nations High Commissioner for Human Rights. The right to privacy in the digital age report. A/HRC/48/31, 13 de septiembre de 2021. Párrafo 45.

contexto de reuniones y protestas pacíficas, ahora para todo tipo de usos estatales del reconocimiento facial[58]:

> ***"Imponer una moratoria sobre el uso de tecnologías de reconocimiento biométrico remoto en espacios públicos, al menos hasta que las autoridades responsables puedan demostrar el cumplimiento de las normas de privacidad y protección de datos y la ausencia de problemas significativos de precisión e impactos discriminatorios***, y hasta que se apliquen todas las recomendaciones establecidas en A/HRC/44/24, párrafo 53 (j) (i - v)"[59]

Esto es, para la OACNUDH debe haber una moratoria del uso del reconocimiento facial, y otros tipos de reconocimiento biométrico, hasta cuando los Estados sean capaces de:

> i) "***practicar la debida diligencia en materia de derechos humanos no solo antes de desplegar los dispositivos de tecnología de reconocimiento facial, sino también durante todo el ciclo de vida útil de esos instrumentos***";
> ii) "Establezcan **mecanismos de supervisión eficaces, independientes e imparciales para la utilización de la tecnología de reconocimiento facial**, como una autoridad independiente de protección de datos, y **consideren la posibilidad de imponer un requisito de autorización previa**, de cuya expedición se encargaría un organismo independiente, para la utilización de las tecnologías de reconocimiento facial en el contexto de las reuniones;
> iii) **Apliquen leyes estrictas de privacidad y protección de datos que regulen la recopilación, retención, análisis y cualquier otro tipo de procesamiento de datos personales, en particular las plantillas faciales**;
> iv) **Velen por la transparencia en el uso de las grabaciones de imágenes y la tecnología de reconocimiento facial en el contexto de las reuniones, entre otras cosas celebrando consultas informadas con**

58 United Nations High Commissioner for Human Rights. Reporte "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas". A/HRC/44/24. Disponible en: https://undocs.org/es/A/HRC/44/24.
59 Op. cit.. Párrafo 59 letra (d)

> **la ciudadanía, los expertos y la sociedad civil**, y proporcionando información sobre la adquisición de la tecnología de reconocimiento facial, los proveedores de dicha tecnología y la precisión de los sistemas;
> v) Cuando recurran a empresas privadas para adquirir o desplegar esas tecnologías de reconocimiento facial, les pidan que practiquen la debida diligencia en materia de derechos humanos para identificar, prevenir, mitigar y abordar los potenciales efectos adversos y reales en los derechos humanos y, en particular, **se aseguren de que se incluyan requisitos de protección de datos y de no discriminación en el diseño y la aplicación de esas tecnologías**".

Los órganos del Sistema Interamericano de protección de los derechos humanos han alineado sus recomendaciones en un sentido similar, si bien no han optado por el llamado directo a la moratoria de uso de estas tecnologías, son claros en las condiciones que deben acompañar a su despliegue:

> *"Entre las acciones que los Estados deben tomar en cuenta se encuentran, por ejemplo,* ***la revisión o adopción de marcos legales claros que faculten y fijen las condiciones de la utilización lícita de este tipo de tecnologías en función de los valores democráticos y las normas de derechos humanos; así como la existencia de salvaguardas de debido proceso, transparencia, fiscalización e investigación independientes y la efectiva rendición de cuentas****. La CIDH y su REDESCA también toman en cuenta información sobre la fragmentación de los sistemas normativos en este ámbito y las debilidades institucionales para que se cumplan aquellas disposiciones vigentes como uno de los mayores desafíos en la región. Igualmente reconocen que existen preocupaciones por la falta de transparencia, e incluso corrupción, y reducidos o nulos espacios de participación social en las instancias estatales que toman decisiones en este ámbito, en particular respecto de adquisición y operación de tecnologías de vigilancia"*[60].

Asimismo, la autoridad Europea de protección de datos durante su más reciente análisis de los desafíos regulatorios que conlleva el despliegue de sistemas de

60 Comisión interamericana de derechos humanos. Informe "Empresas y Derechos Humanos: Estándares Interamericanos", Relatoría Especial sobre Derechos Económicos Sociales Culturales y Ambientales, 2019, párrafo 283, https://www.oas.org/es/cidh/informes/pdfs/EmpresasDDHH.pdf.

IA optó también por hacer un llamado de moratoria de uso de reconocimiento automatizado de características humanas en espacios de acceso público y algunos otros usos de la inteligencia artificial que pueden conducir a una discriminación injusta, señalando a este respecto:

> *"La identificación biométrica remota de personas en espacios de acceso público plantea un alto riesgo de intrusión en la vida privada de las personas, con graves efectos en la expectativa de la población de permanecer en el anonimato en los espacios públicos. Por estas razones, el EDPB-EDPS piden una prohibición general de cualquier uso de IA para un* ***reconocimiento automatizado de rasgos humanos en espacios de acceso público, como rostros,*** *pero también de marcha, huellas dactilares, ADN, voz, pulsaciones de teclas y otras señales biométricas o de comportamiento, en cualquier contexto. A la prohibición se recomienda igualmente en los sistemas de inteligencia artificial que clasifican a las personas desde la biometría en grupos. según la etnia, el género, así como la orientación política o sexual, u otros motivos de discriminación en virtud del Artículo 21 de la Carta [europea de derechos humanos]. Además, el EDPB-EDPS consideran que el El uso de IA para inferir las emociones de una persona física es altamente indeseable y debería prohibirse"*[61].

Finalmente, la Resolución sobre "El derecho a la privacidad en la era digital" del Consejo de Derechos Humanos del año 2021, adoptada el 7 de octubre de 2021, recoge una vez más la experiencia del sistema internacional de los derechos humanos en relación con la afectación de derechos fundamentales a través de tecnologías digitales, incluida la inteligencia artificial y los propósitos tales como la identificación biométrica automatizada. Al respecto, el informe señala:

> "Reconociendo *que, a pesar de sus efectos positivos, el uso de intelgencia artificial que requiere el procesamiento de grandes cantidades de datos, a menudo relacionados con datos personales, incluido el comportamiento de un individuo, sus relaciones sociales, sus preferencias privadas y su*

61 EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 de junio 2021, disponible en: https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

*identidad, puede suponer serios riesgos al derecho a la privacidad, en particular cuando se utiliza para la identificación, rastreo, perfilamiento, reconocimiento facial, predicción de comportamiento o la clasificación (*scoring*) de personas.*

"Notando con preocupación *los informes que muestran una menor precisión de las tecnologías de reconocimiento facial con ciertos grupos, en particular individuos no blancos y mujeres, incluyendo cuando se utilizan datos de entrenamiento no representativos, que el uso de tecnologías digitales puede reproducir, reforzar e incluso exacerbar desigualdad racial, y en este contexto la importancia de remedios efectivos".*[62]

En cuanto a sus recomendaciones, mediante la Resolución, el Consejo de Derechos Humanos:

"*Exhorta a todos los Estados:*

(a) A respetar y proteger el derecho a la privacidad, incluido en el contexto de las comunicaciones digitales y tecnologías digitales nuevas y emergentes;

(b) A adoptar medidas para terminar con las violaciones y abusos al derecho a la privacidad y a crear las condiciones para prevenir tales violaciones y abusos, incluso asegurando que la legislación nacional relevante cumpla con sus obligaciones bajo el derecho internacional de los derechos humanos; (…)

(e) A asegurarse de que la identificación biométrica y las tecnologías de reconocimiento, incluidas las tecnologías de reconocimiento facial por actores públicos y privados no faciliten la vigilancia arbitraria o ilícita, incluida la de quienes ejercitan su derecho a la libertad de reunión pacífica; (…)

(k) A abstenerse del uso de tecnologías de vigilancia de una manera no consistente con las obligaciones de derecho internacional de los derechos humanos, incluido cuando se usa contra periodistas y defensores de derechos humanos, y adoptar acciones específicas para la protección contra violaciones del derecho a la privacidad, incluso mediante la regulación de la venta, transferencia, uso y exportación de tecnologías de vigilancia"[63].

62 Consejo de Derechos Humanos, "The right to privacy in the digital age", A/HRC/48/L.9/Rev.1, adoptado por consenso el 7 de octubre de 2021, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G21/274/69/pdf/G2127469.pdf?OpenElement (traducción propia por no haber texto oficial en español a la fecha)

63 Ibid.

Con ocasión de la aprobación de la Resolución antedicha, el propio Estado argentino ha reafirmado la importancia del derecho a la privacidad y los riesgos asociados a la identificación biométrica. En la ocasión, el representante de Argentina enfatizó que "el derecho a la privacidad es un derecho de guardián (*gatekeeper*) que permite el disfrute de otros derechos, como de asociación y de reunión", y recordó que "se ha demostrado que el reconocimiento facial es menos preciso en rostros que no son blancos"[64]. De este modo, es el propio Estado argentino el que ha reafirmado tanto las deficiencias de estas tecnologías como sus riesgos sobre los derechos humanos de las personas.

En suma, existe una experiencia vasta en el sistema internacional de protección de derechos a diferentes niveles globales y regionales en que la constatación de los riesgos de los sistemas de reconocimiento facial desplegados en espacios públicos para el ejercicio de los derechos fundamentales que han sido identificados en estos autos les hacen concluir la necesidad de que ellos sean analizados en la forma más estricta en su despliegue técnico y jurídico, y si no en todos los casos prohibirlos, cuando no se encuentren acompañados de las condiciones que aquí han sido expuestas que claramente no se satisfacen por el SRFP objeto de la presente acción de constitucionalidad.

9. Personería y representación

Juan Carlos Lara y Paula Jaramillo actúan en nombre y representación legal de Derechos Digitales mediante habilitación estatutaria que consta de la escritura de 7 de septiembre de 2021 otorgada ante el Notario Interino de la Décimo Cuarta Notaría de Santiago de Chile, don Jorge Andrés Osorio Rojas. El mandato especial que confiere poder en la causa a la Dra. María Soledad Marinaro consta de escritura pública de 27 de septiembre de 2021, otorgada ante el Notario Titular de la Primera Notaría de Providencia, Santiago de Chile, don Luis Eduardo Rodríguez, Repertorio Nº 5186-2021. Declaramos bajo juramento que el poder mencionado se encuentra plenamente vigente y sin limitaciones de ninguna naturaleza. En base a ello, solicito se tenga por presentada la petición y por acreditada la personería y la representación en la

64 Consejo de Derechos Humanos, “41st Meeting, 48th Regular Session Human Rights Council” https://media.un.org/en/asset/k19/k19oisdczr

presente causa.

10. Petitorio

Por todo lo expuesto, a V.E. se solicita: que se tenga a Derechos Digitales presentados como “amigos del tribunal”, como así también que los argumentos aportados sean utilizados para la resolución del caso y se provea favorablemente la presentación de la parte actora.

PROVEER DE CONFORMIDAD
SERÁ JUSTICIA

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 PRESENTA COMO AMIGOS DEL TRIBUNAL

Con los siguientes adjuntos:
documental DD.pdf

FIRMADO ELECTRONICAMENTE 12/10/2021 16:03:13

MARINARO MARIA SOLEDAD - CUIL 27-23004423-1