Ciudad Autónoma de Buenos Aires, 14 de octubre de 2021

SE PRESENTAN EN CALIDAD DE AMICUS CURIAE

Sr juez:

Beatriz Busaniche, DNI 21.737.845 en mi caracter de presidenta de Fundación Vía Libre, con el patrocinio letrado de la Dra 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, con domicilio real en calle Roosevelt Nº 3907 de la Ciudad Autónoma de Buenos Aires, en la causa "OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO O.D.I.A. CONTRA GCBA SOBRE AMPARO - OTROS", EXPTE N° 182908/2020-0, que tramita ante vuestro tribunal, me presento y respetuosamente digo:

I. OBJETO

1. Vengo a presentar éste documento, como presidenta y en representación de la Fundación Vía Libre, de amicus curiae con la finalidad de exponer nuestra opinión como expertos en materia del impacto de las tecnologias cuestionadas en esta causa en los derechos humanos, del cual hace más de 20 años de trayectoria que versamos en la protección de derechos como la privacidad, intimidad y reunión. Derechos que se encuentran enumerados de forma directa en este expediente judicial.

II. LEGITIMACIÓN

2. Fundación Vía Libre es una organización en torno a las tecnologías informáticas y la utilización de software libre, la defensa de los derechos humanos en entornos digitales. Nuestro objeto es promoveer la libertad de las personas, grupos, asociaciones, comunidades, fundaciones, empresas de acceder, difundir, estudiar, desarrollar, mejorar el conocimiento en general, y de esta manera promover el moejoramiento económico y socialde los grupos antes mencionados: promover la capacitación, el crecimiento, la organización y el desarrollo sostenido de grupos, asociaciones, fundaciones, empresas, sean estas urbanas o rurales permitiendo el acceso de éstasa los beneficios de la sociedad global; fomentar y difundir las actividades de estudios e investigación y desarrollo en todas las ramas de las ciencias, la cultura y las artes en general para cumplir los objetivos antes mencionados, la creación, difusion y creación de Software Libre sin que esto constituya limitante alguno para lograr los fnes mencionados en nuestro Estatuto Constitutivo.

3. Amicus Curiae. En nuestra realidad jurídica se encuentra incorporado y con gran aceptación la figura del amicus curiae, vinculada con antecedentes en el derecho internacional de derechos humanos, siendo reconocida por nuestros tribunales nacionales e internacionales. A nivel nacional encuentra su base en el art 33 de la CN. La Corte Suprema de Justicia no solo toma como fundamento nuestra CN sino que reconoce ,conforme el art 36 del CPCCN, la escucha de opiniones de entidades o personas que no son parte del proceso a los fines de aportar una opinión vinculante y legitimada al caso.

4. La regulación de la Corte suprema a través del dictado de la acordada 28/2004, en la cual admite la posibilidad de presentar amicus curiae ante la CSJN, da cuenta de que no debería haber rechazos en instancias inferiores. En los considerandos de dicha acordada se indica: *“en el marco de las controversias cuya resolución por esta Corte genere un interés que trascienda al de las partes y se proyecte sobre la comunidad o ciertos sectores o grupos de ella, a fin de resguardar el más amplio debate como*

2https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

garantía esencial del sistema republicano democrático, debe imperar un principio hermenéutico amplio y de apertura frente a instituciones, figuras o metodologías que, por su naturaleza, responden al objetivo de afianzar la justicia entronizado por el Preámbulo de la Constitución"

5. Luego a través de la acordada 7/2013 con respecto a amicus curiae manifiesta:"pluralizar y enriquecer el debate constitucional, así como de fortalecer la legitimación de las decisiones jurisdiccionales dictadas por esta Corte Suprema en cuestiones de trascendencia institucional". Ésta acordada que regula sobre la presentación de Amigos del Tribunal tiene establecido que pueden presentarse personas -físicas o jurídicas- en calidad de Amigos del Tribunal en "todos los procesos judiciales correspondientes a la competencia originaria o apelada en los que se debatan cuestiones de trascendencia colectiva o interés general".
6. Conforme a lo expuesto a los fines de que mi opinión pueda resultar útil en ésta causa al momento de dictar sentencia, es que vengo a presentarme en calidad de AMICUS CURIAE

III. RESUMEN DEL CASO Y EJE DE LA INTERVENCIÓN

7. La presente causa es una Acción de Amparo Colectivo presentada por el OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.) contra el GOBIERNO DE LA CIUDAD DE BUENOS AIRES, por el uso de sistemas de vigilancia masiva.
8. Dicho acción sostiene que los actos administrativos y modificaciones regulatorias que hacen al Sistema de Reconocimiento Facial de Prófugos, el Sistema Preventivo y el Sistema Forense, las bases de datos y la infraestructura para su funcionamiento, son violatorios de derechos humanos consagrados por la Constitución Nacional y por los Tratados Internacionales.
9. Asimismo, se solicita medida cautelar de no innovar En la misma demanda se solicita una medida cautelar de no innovar, establecida en el art. 15 de

3https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

la Ley Nº 2.145 y concordantes a fin de que V.S. ordene la inmediata suspensión sobre el acto administrativo Resolución N° 398/MJYSGC/19 y los siguientes artículos de la Ley Nº 6.339 que modifica la ley Nº 5.688 en sus artículos 478, 480, 483, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis, a fin de evitar los graves perjuicios que la aplicación inmediata de estos artículos provoca.

IV. CONSIDERACIONES PRELIMINARES: SISTEMAS DE RECONOCIMIENTO FACIAL.

10. Las tecnologías de reconocimiento facial o reconocimiento automatizado de características humanas interfieren con el derecho a la intimidad, pero su impacto se extiende mucho más allá de este derecho fundamental. Su aplicación, como en cualquier circunstancia en que se empleen métodos automatizados para acciones que incidan negativamente en el ejercicio de derechos fundamentales, debe estar sujeta a adecuado control jurisdiccional, pero además debería llevarse a cabo solo después de una exhaustiva verificación de cumplimiento de los principios de necesidad, legalidad y proporcionalidad. Ahora bien, las tecnologías a las que aquí nos referimos no solo resultan invasivas de la esfera privada sino también conllevan riesgos de grave error y tienden a producir indeseados efectos intimidatorios en la sociedad.
11. Los sistemas de reconocimiento facial son probabilísticos, es decir que no producen respuestas binarias “sí” o “no” sino que identifican coincidencias más o menos probables. Como todo algoritmo informatizado, los algoritmos de reconocimiento facial no son generadores de verdad neutrales e infalibles, sino que “varían en su capacidad de identificar personas, y ningún sistema es cien por ciento exacto bajo todas las condiciones”.[1] La

1 Lynch, Jennifer. 2018. *Face Off: Law Enforcement Use of Face Recognition Technology. Electronic Frontier Foundation*. Disponible en línea en

https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

exactitud del reconocimiento es afectada directamente por la calidad de las imágenes sobre las que se realiza la búsqueda; cuando dos imágenes contienen iluminación, sombras, fondos, poses o expresiones diferentes se verá afectada la exactitud;[2] la capacidad de identificación puede ser muy pobre cuando se trata de imágenes de baja resolución[3] o video,[4] o cuando la búsqueda se realiza contra una base de imágenes muy grande, en parte debido a que muchas personas dentro de una población dada tienen apariencias similares.[5] Todas estas variables reducen la exactitud en la búsqueda y comparación.

12. Estos errores —y las altas tasas de falsos positivos y falsos negativos que son su consecuencia— resultan exacerbados cuando los algoritmos se emplean sobre imágenes de ciertos grupos demográficos. La tasa de exactitud de los sistemas de reconocimiento facial está estrechamente vinculada con los datos (es decir, las imágenes de rostros) usados para entrenarlos.[6] Los sistemas "aprenden" cómo identificar rostros analizando imágenes previamente identificadas en un conjunto de datos de

<https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf>

2 Véase, por ejemplo, Phillips, P.J.; Beveridge, J.R; Draper, B.A.; et al. 2011. *An Introduction to the Good, the Bad, & the Ugly Face Recognition Challenge Problem*. NIST Interagency/Internal Report (NISTIR) 7758. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.IR.7758.

3 Véase, por ejemplo, Yang, Min-Chun; et al. 2015. "Recognition at a Long Distance: Very Low Resolution Face Recognition and Hallucination". *IEEE 2015 International Conference on Biometrics*, pp. 237–42.

4 Véase, en general, Grother, Patrick; Quinn, George; y Ngan, Mei. 2017. *Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects*. NIST Interagency/Internal Report (NISTIR) 8173. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.IR.8173.

5 Véase, por ejemplo, LaFrance, Adrienne. 2016. "The Ultimate Facial-Recognition Algorithm". *The Atlantic*, 28/6/2016.

6 Véase, entre otros, Klare, Brendan; Burge, Mark; Klontz, Joshua; et. al. 2012. "Face Recognition Performance: Role of Demographic Information". *IEEE Trans. on Information Forensics and Security* **7**(6):1789-1801. DOI: 10.1109/TIFS.2012.2214212; Boulamwini, Joy y Gebru, Timnit. 2018. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". Proceedings of the 1st Conference on Fairness, Accountability and Transparency, *Proceedings of Machine Learning Research* **81**:77-91 (disponible en línea en <https://proceedings.mlr.press/v81/buolamwini18a.html>.

5https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

entrenamiento. Si las imágenes de ese conjunto no representan a la población que el sistema estará en definitiva destinado a identificar, entonces su exactitud disminuye significativamente. Este es un problema de la mayoría de los algoritmos de reconocimiento facial usados en la actualidad. Sus conjuntos de entrenamiento "están compuestos típicamente de celebridades" lo que "hace más fácil etiquetar miles de rostros individuales, pero falla en capturar el rango completo de la diversidad humana".[7] Un estudio del Massachusetts Institute of Technology (MIT) halló que dos conjuntos de datos utilizados para entrenar algoritmos de reconocimiento facial estaban "abrumadoramente compuestos de sujetos de piel clara".[8] Se introducen sesgos adicionales cuando los sistemas de reconocimiento facial se basan en imágenes de cámaras digitales porque cuando se toman fotografías de rostros de piel más oscura estas cámaras fallan en proporcionar el grado de contraste de color que los algoritmos necesitan para producir y correlacionar impresiones faciales.[9] Diversos investigadores han reportado que los algoritmos de reconocimiento facial identifican incorrectamente a personas de piel oscura, jóvenes y mujeres con mayor frecuencia que a personas de piel clara, de mayor edad y hombres, respectivamente.[10] En una prueba llevada a cabo en 2018 un algoritmo de reconocimiento facial difundido entre organismos de seguridad pública, puesto en su configuración por defecto, correlacionó falsamente a 28 miembros del Congreso de los Estados Unidos con fotografías de una base de datos de detenidos.[11] Cabe notar que mientras que las personas de color constituyen normalmente un 20% del Congreso estadounidense, representaron un 40% de los resultados erróneos arrojados por el algoritmo.

13. Aún cuando haya intervención humana en la revisión de los resultados del

7 Garvie, Clare; Bedoya, Álvaro; Frankle, Jonathan; et al. 2016. *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Washington, DC: Georgetown Law - Center on Privacy and Technology. pp. 50-51.
8 Buolamwini y Gebru, cit. *supra*.
9 Garvie, cit. *supra*, p. 54.
10 Véanse, por ejemplo, las fuentes citadas en Klare y en Boulamwini, *supra*.
11 Snow, Jacob. 2018. "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots". *ACLU Free Future*, 26/7/2018.

6https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

algoritmo, esta revisión puede fallar en subsanar una identificación errónea. Investigaciones llevadas a cabo por el National Institute of Standards and Technology de los Estados Unidos y otros muestran que las personas generalmente tienden a creer en los resultados generados por computadora, y que aquellas que no están especialmente entrenadas en reconocimiento de rostros suelen errar al identificar personas que no conocen,[12] aún si realizar estas identificaciones es parte de su trabajo diario.[13] Hasta los especialistas entrenados producen identificaciones erróneas alrededor de un 10% de las veces.[14]

14. Resulta de particular interés, por las similitudes de método y propósito que tienen con el sistema empleado en la ciudad de Buenos Aires, el análisis independiente realizado en 2019 por la Universidad de Essex sobre ensayos de reconocimiento facial en vivo (LFR, por su sigla en inglés) realizados por la Policía Metropolitana de Londres durante 2018 y 2019.[15] Como en el caso de la ciudad de Buenos Aires, estos sistemas procuraban identificar imágenes de rostros tomadas por cámaras de video en vivo contra imágenes estáticas de una lista de personas buscadas. En caso de una coincidencia positiva de identificación generada por el sistema, el resultado era presentado a un operador humano ("adjudicator") para confirmar o descartar la coincidencia y en caso de confirmación se producía la intervención policial en el terreno. Los resultados de las seis pruebas observadas de principio a fin por los investigadores muestran que en el 80.95% de los casos la coincidencia generada por el sistema resultó ser un

12 Véase, entre otros, Phillips, P.J.; Yates, A.N.; Hu, Y.; et al. 2018. "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms". Proceedings of the National Academy of Sciences **115**(24):6171-6176. DOI: 10.1073/pnas.1721355115; White, D.; Dunn, J.D.; Schmid, A.C.; Kemp, R.I. 2015. "Error Rates in Users of Automatic Face Recognition Software". *PLoS ONE* **10**(10): e0139827. DOI: 10.1371/journal.pone.0139827

13 White, et al., Error Rates, cit. *supra*, hallando rendimiento equivalente entre examinadores no entrenados y agentes de control de pasaportes.

14 Phillips, Face Recognition Accuracy, *supra*.

15 Fussey, Pete y Murray, Daragh. 2019. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. Colchester: Human Rights Centre, University of Essex.

https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

falso positivo. En otros términos, cuatro de cada cinco personas identificadas por el sistema como pertenecientes a la lista de buscadas no lo eran. El proceso de revisión humana probó ser de alguna utilidad, porque los 'adjudicators' descartaron el 38.1% de los casos presentados como coincidencia por el sistema, pero aún con este control adicional casi dos tercios de las personas interpeladas en la vía pública por la policía resultaron en falsas identificaciones positivas. Dadas las características de los ensayos, resulta imposible determinar la proporción de falsos negativos, es decir los casos en que personas que aparecían entre las buscadas fueron captadas por las cámaras pero no reconocidas como coincidencia.

15. Los resultados de la mencionada investigación de Fussey y Murray son, en términos generales, coherentes con los obtenidos por Davies, Innes y Dawson de la Universidad de Cardiff respecto del uso de reconocimiento facial automatizado por la policía del Sur de Gales.[16] Cabe recordar que el despliegue masivo de un sistema de reconocimiento facial (NeoFace Watch, provisto por la multinacional NEC) durante la final del año 2017 de la Champions League en Cardiff resultó en un elevado nivel de error: las coincidencias positivas correctas fueron apenas el 7% de las determinadas por el sistema.[17] Del trabajo de Davies et al. resulta razonable concluir que el despliegue de sistemas de reconocimiento facial en contextos de gran circulación de personas es proclive a grueso error, y que los resultados varían sensiblemente dependiendo del grado de similitud establecido para que el algoritmo de reconocimiento dispare un aviso de coincidencia.

16. Las amenazas para los derechos fundamentales que supone la utilización de reconocimiento facial ha llevado a que en los últimos años una cantidad creciente de cuerpos legislativos discutieran medidas para regular la tecnología.

16 Davies, Bethan; Innes, Martin y Dawson, Andrew. 2018. *An Evaluation of South Wales Police's Use of Automated Facial Recognition*. Cardiff: Crime and Security Research Institute, Cardiff University.

17 Véase, por ejemplo, Burgess, Matt. 2018. “Facial recognition tech used by UK police is making a ton of mistakes”. *Wired*, 5 abr 2018. Disponible en línea en <https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival>

8https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

17. A título de ejemplo, en los Estados Unidos de América el reconocimiento facial en espacios públicos ha sido prohibido o puesto en moratoria indefinida en Alameda, estado de California, desde el 17 de diciembre 2019, por voto unánime del consejo municipal; Berkeley, California, desde el 16 de octubre de 2019, prohibiendo todo uso de reconocimiento facial por organismos gubernamentales; Boston, Massachusetts, desde el 24 de junio 2020; Brookline, Massachusetts, desde el 11 de diciembre 2019; Cambridge, Massachusetts, desde el 13 de enero 2020, vedando todo uso de reconocimiento facial a los organismos públicos de la ciudad e incluyendo cualquier información obtenida mediante dicha tecnología; Jackson, Missouri. desde el 20 de agosto 2020, prohibiendo el uso policial de tecnologías de reconocimiento facial; King County, Washington (condado que incluye a la ciudad de Seattle, uno de los polos de desarrollo de tecnologías de información en los EE. UU. y sede de los notorios desarrolladores de reconocimiento facial Amazon y Microsoft), a partir del 1 de junio 2021; en la ciudad de Madison, capital del estado de Wisconsin, desde el 1 de diciembre 2020; Minneapolis, Minnesota, desde el 12 de febrero 2021, por voto unánime del consejo municipal — en parte como respuesta al asesinato de George Floyd por un agente policial en la ciudad, en el verano de 2020; New Orleans, Louisiana, desde el 17 de diciembre de 2020, prohibiendo asimismo el uso de técnicas de "policialización preventiva"; Northampton, Massachusetts, desde el 19 de diciembre 2019, resolviendo por unanimidad del consejo municipal la prohibición de recolectar y usar información biométrica recogida mediante tecnologías de vigilancia; Oakland, California, desde el 16 de julio 2019; Pittsburgh, Pennsylvania, desde el 22 de septiembre 2020; Portland, Maine, desde el 3 de agosto 2020, ratificada por un referendum del 2 de noviembre; Portland, Oregon, desde el 9 de septiembre 2020, prohibiendo adicionalmente el uso de la tecnología de reconocimiento facial en los espacios privados accesibles al público; San Francisco, California, desde el 14 de mayo de 2019 (la primera ciudad de los Estados Unidos en establecer la prohibición); Somerville, Massachusetts, desde el 27 de junio de 2019; Springfield, Massachusetts, desde el 4 de febrero 2020, estableciendo una moratoria indefinida.

9https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

18. El estado de Vermont promulgó el 7 de octubre 2020 una moratoria indefinida (S.124) en el uso de tecnologías de reconocimiento facial o cualquier información resultante de ellas por las fuerzas policiales. El estado de Virginia estableció en abril de 2021, con vigencia a partir del 1 de julio 2021, lo que en la práctica es una prohibición *de facto* (HB2031): se veda el uso de reconocimiento facial a todo departamento de policía en el estado si no cuenta con previa aprobación expresa de la Legislatura. El estado de Maine sancionó en junio de 2021, con vigencia a partir del 1 de octubre 2021, la norma LD1585 que prohíbe a los organismos públicos del estado, condados y municipios, y a sus funcionarios, el uso o posesión de tecnologías de reconocimiento facial o la celebración de acuerdos con terceros para obtener la tecnología, lograr acceso a ella o hacer uso de la misma. La ley establece también derechos de las personas sujetas a la jurisdicción del estado para obtener medidas cautelares contra el uso de reconocimiento facial por funcionarios públicos y sanciones aplicables a los funcionarios que violen la norma, y determina que los resultados de un reconocimiento facial no son por sí mismos suficientes para justificar detenciones ni allanamientos.
19. Hace apenas unos días el Parlamento Europeo aprobó la iniciativa 2020/2016(INI) *Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales*,[18] instando a los Estados miembros de la Unión Europea a prohibir el uso de reconocimiento facial en espacios públicos, como así también las bases de datos de reconocimiento facial privadas (como por ejemplo la de Clearview AI en uso por algunas fuerzas de seguridad) y las técnicas de policialización preventiva basadas en datos de comportamiento. Sin perjuicio del análisis que V.S. haga de la extensa Resolución de referencia, nos permitimos destacar el considerando “O”, que transcribimos: “el uso de la IA en el ámbito de la garantía del cumplimiento de la ley entraña riesgos potencialmente elevados y en ocasiones inaceptables para la protección de los derechos fundamentales de las personas, como la opacidad en la toma

18 Disponible en su versión oficial en español en <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html>

10https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

de decisiones, diferentes tipos de discriminación y errores inherentes al algoritmo subyacente que pueden verse reforzados por bucles de retroalimentación, así como riesgos para la protección de la privacidad y los datos personales, la protección de la libertad de expresión y la información, la presunción de inocencia, el derecho a tutela judicial efectiva y a un juez imparcial, y riesgos para la libertad y la seguridad de las personas". Transcribimos también, por cuanto es de especial interés para la materia bajo juzgamiento, parte del punto dispositivo 31 de la Resolución: "[el Parlamento] pide, por consiguiente, a la Comisión que, por medios legislativos y no legislativos y si es necesario a través de procedimientos de infracción, aplique una prohibición de cualquier tratamiento de datos biométricos, incluidas las imágenes faciales, con fines coercitivos que dé lugar a una vigilancia masiva en espacios públicos".

20. Esta Resolución del Parlamento Europeo es consonante con la Opinión Conjunta 5/2021[19] de 18 de junio 2021 del Comité Europeo de Protección de Datos (el organismo conjunto de las autoridades de protección de datos personales de los estados de la Unión) y el Supervisor Europeo de Protección de Datos, cuyo párrafo 32 "llama a una prohibición general de cualquier uso de inteligencia artificial para el reconocimiento automatizado de características humanas en espacios públicamente accesibles —tales como rostros pero también andar, huellas dactilares, ADN, voz, tecleo y otras señales biométricas o de comportamiento— en cualquier contexto" y cuyo párrafo 33 "recomienda una prohibición, tanto para autoridades públicas cuanto entidades privadas, de sistemas de inteligencia artificial que caractericen a las personas a partir de la biometría (por ejemplo, por reconocimiento facial) en grupos conformes a us etnicidad, género, así como orientación sexual o política, u otras bases de discriminación prohibidas bajo el Artículo 21 de la Carta [de los Derechos Fundamentales de la Unión Europea]".

21. En síntesis, y con base en los elementos de juicio precedentemente

19 Disponible en su versión original en inglés en <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf>.

11 https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

expuestos, es nuestra conclusión que V.S. debe hallar que el sistema de reconocimiento facial empleado por el gobierno de la Ciudad de Buenos Aires excede los límites razonables de restricción a las libertades individuales, y por lo tanto infringe derechos fundamentales consagrados en el texto constitucional.

V. DERECHOS SOBRE LOS DATOS PERSONALES.

22. Para abocarnos a estos puntos nos hemos permitido solicitar la colaboración del Instituto de Ciencias de la Computación – CONICET desde el cual el Dr Pablo Negri (Investigador CONICET), la Dra Vaninna Martinez (Investigadora CONICET) y el Dr Sebastián Uchitel (Director del Instituto de Ciencias de la Computación de la Universidad de Buenos Aires – CONICET) nos manifiestan por escrito:

ICC Instituto de Ciencias de la Computación

Reconocimiento facial en cámaras ciudadanas: se desaconseja su uso

El reconocimiento facial (RF) se ha propuesto repetidas veces como forma de monitoreo y vigilancia en la vía pública, especialmente en zonas donde transitan muchas personas. Específicamente relacionado al "policiamiento" basados en estos sistemas, si bien pueden, en teoría, agilizar y optimizar la forma de detectar personas que estén siendo buscadas por la justicia, **los riesgos que la incorporación de esta tecnología introduce parecen ser demasiado importantes en contraposición con el beneficio que podrían otorgar**.

En los últimos años, los sistemas de RF han sido objeto de muchas controversias, especialmente enfocadas en cuestiones de privacidad, sesgo, y violación de derechos y

12 https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

libertades civiles. En este documento intentaremos abordar con argumentos técnicos algunos de los riesgos que se han identificado.

Riesgos de privacidad y uso dual de la tecnología

La tecnología de reconocimiento facial en la vía pública puede resultar una invasión de la privacidad y no existe ni reglamentación que garantice que se utilice correctamente, ni marco legal de rendición de cuentas apropiado cuando este no sea el caso.

La introducción de sistemas informáticos en procesos que manipulan información sensible o datos protegidos, o que están involucrados en el apoyo de toma de decisiones que puedan resultar en perjuicio de los derechos humanos y legales establecidos conlleva numerosos riesgos inherentes.

Desde un punto de vista práctico se conoce que es relativamente fácil vulnerar o manipular los sistemas de información, lo que en el caso de vigilancia en base a técnicas de RF podría llevar a utilizarlos como un arma contra civiles inocentes o personas críticas con los organismos que lo utilizan. Si bien es posible implementar mecanismos para mitigar este tipo de problemas, es imposible eliminar por completo este tipo de vulnerabilidades, muchas veces independientemente de que se implementen estándares y buenas prácticas de seguridad informática, e incluso cuando existan marcos regulatorios y legales adecuados para prevención, auditoria y rendición de cuentas. Cabe aclarar que a nivel local no existen dichos marcos legales ni regulaciones que aseguren la calidad de los sistemas informáticos en general.

Además, en los sistemas de RF, la superficie de ataque, es decir los puntos donde el sistema puede ser objeto de un ataque malintencionado, se amplía considerablemente, en relación con otros sistemas de información. Un claro ejemplo de esto son los potenciales ataques por “envenenamiento” de datos, tanto en la etapa de entrenamiento del sistema corrompiendo el conjunto de datos, como en la alteración de la señal de entrada en los dispositivos de captura de imágenes en tiempo real. Estos son todos problemas abiertos para los cuales no se tienen aún soluciones técnicas efectivas.

13 https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

Consideraciones sobre el desempeño

Los algoritmos de reconocimiento (de cualquier tipo, no sólo facial) se evalúan en términos de precisión y exhaustividad; la precisión representa cuántos de los resultados positivos son sobre individuos de la clase a reconocer (qué tan poco reconoce "de más" el sistema), y la exhaustividad representa cuántos de los individuos de la clase a reconocer son efectivamente reconocidos (qué tan poco reconoce "de menos" el sistema). Se da entre estas dos métricas una relación de compromiso: si el algoritmo da un resultado positivo *siempre*, su precisión será muy poca pero su exhaustividad será perfecta, mientras que si no lo da nunca su precisión será perfecta pero su exhaustividad será nula.

Vale decir, que aumentar la precisión es posible, pero a partir de cierto nivel tiene un costo en términos de exhaustividad, y viceversa. Cuando tenemos que la mayor parte de las personas que pasan frente a una cámara no está siendo buscada por el sistema (debe dar un resultado negativo), una tasa pequeña de falsos positivos se refleja de todas formas en una gran cantidad de éstos, por ser la mayor parte de los transeúntes “negativos”. Si ajustamos el sistema para que no haya falsos positivos, lo que sucederá es que el sistema no detectará a buena parte de los pocos que sí busca.

La publicación Chequeado.com[20] publicó un documento sobre la video vigilancia en 2020. En él se lee:

> *“En el Reino Unido, el RF es aplicado por las policías de Londres y Gales del Sur. Allá, la efectividad de los algoritmos de RF para reconocer los rostros de personas buscadas también fue objetada. En el primer caso, la Universidad de Essex hizo una auditoría sobre los procedimientos e impacto en derechos humanos en seis de las diez pruebas piloto de esta tecnología que la Policía realizó en eventos y espacios públicos entre 2016 y 2019. Publicado a mitad del año último, sus conclusiones fueron críticas. De 42 “coincidencias” de rostros que arrojó el sistema sobre la base de datos de personas buscadas, sólo 8 pudieron ser verificadas como correctas (apenas un 19% de efectividad). Y el 63,64% de las personas que fueron detenidas en la vía pública para chequear su identidad luego de una alerta del sistema, se trató de un falso positivo.*
>
> *En el mismo sentido, una auditoría de la Universidad de Cardiff sobre el uso de*

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

https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

esta tecnología por parte de la Policía del Sur de Gales en eventos que tuvieron lugar entre junio de 2017 y marzo de 2018, encontró que los "falsos positivos" -posible coincidencia que sugiere el sistema, pero que un operador humano desestima por evaluarla incorrecta- corresponden al 72% del total de casos, que posteriormente una nueva versión del algoritmo bajó al 50%. En tanto, los "verdaderos positivos" -posible coincidencia generada por el sistema que los operadores humanos consideran correcta- fueron del 3% y el 46% en cada caso."

Es importante entender que los resultados de estos mecanismos de evaluación de desempeño son relativos a los conjuntos de datos particulares con los que se desarrollan estos sistemas y no pueden generalizarse o extrapolarse directamente a otras poblaciones. Muchos de estos resultados son preliminares, tanto positivos como negativos, lo cual nos puede dar una idea bastante lejana de cómo se comportarán esos sistemas una vez inmersos en el mundo real (fuera del laboratorio) en situaciones altamente cambiantes y probablemente no anticipadas. Por otro lado, no contamos actualmente con protocolos que nos permitan evaluar estos sistemas de manera exhaustiva y efectiva sin ponerlos en práctica, es decir enfrentándolos a los entornos reales de uso y, para el caso de RF, aplicados a la población autóctona.

Antecedentes de oposición de la comunidad científica y tecnológica

En el 2020 el Comité de Política Tecnológica de la ACM (Asociación para Maquinaria de Computación, uno de los organismos científicos más importantes a nivel mundial en temas informáticos, encargado entre otras cosas de otorgar el premio equivalente al Nobel que tiene la disciplina) publicó un reporte[21] donde evalúa el estado actual de las tecnologías de reconocimiento facial. El Comité concluye, luego de un proceso de evaluación riguroso, que esta tecnología muy a menudo produce resultados que demuestran un claro sesgo basado en la etnia, la raza, el género, entre otras características humanas reconocibles por los sistemas informáticos, por lo que su utilización no sólo no es aconsejable sino que con frecuencia puede extenderse a provocar daños profundos y afectar los derechos fundamentales de las personas, sobre todo poblaciones vulnerables. A partir de estas conclusiones aconsejan la suspensión inmediata, tanto de forma privada como gubernamental, de tecnologías de RF en todas las circunstancias conocidas o razonablemente previsible que sea perjudicial para los derechos humanos y legales establecidos.

21 https://www.acm.org/media-center/2020/june/ustpc-issues-statement-on-facial-recognition-technologies

15 https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

Algunas empresas internacionales como Amazon, Microsoft e IBM han optado por reconsiderar sus posturas sobre su desarrollo y ventas de este tipo de sistemas a las agencias de policiamiento y de fuerzas del orden como se puede ver en el artículo "Big tech companies back away from selling facial recognition to police. That's progress."[22]

Conclusiones

A partir de lo expuesto, puede verse que por el momento no hay:

- Legislación nacional que dé un marco seguro y consensuado para el uso de RF.
- Condiciones técnicas para asegurar el monitoreo que prevenga efectivamente abusos, dado que con la tecnología actual son muy fáciles de cometer y que pasen desapercibidos hasta que sus consecuencias sean ostensibles y por ende graves.
- Consenso internacional sobre que las tecnologías de RF en la vía pública hayan llegado a un grado de madurez que permita su uso seguro.

Por lo tanto, la recomendación técnica es que no se proceda a su uso.

Por lo expuesto

23. Solicitamos se nos tenga por legitimado y presentado como amicus curiae y que V.S tenga en cuenta:
24. que la utilización de cámaras de reconocimiento facial por parte del estado, por el cual puede monitorear y controlar vastos espacios públicos e identificar las personas que circulan en ellos, nos remite inequívocamente a la vigencia del espacio público sucedida en los peores momentos de nuestra historia reciente. [23]

22

23 Mereb, A. (2018). Control político y vigilancia militar durante la última dictadura en la Argentina. Aportes desde una mirada microhistórica en El Bolsón, Río Negro. Revista Pilquen-Sección Ciencias Sociales, 21(4), 22-31.

16https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

25. El peligro implícito en la utilización de esta tecnología supera con creces las ventajas que la misma pretende brindar a la sociedad.
26. El riesgo real que conlleva a la discriminación sobre las minorías a las cuales integramos.

VII. PERSONERIA

Que con la constancia que adjunto vengo acreditar con el acta fundacional la constitución de la asociación y con el acta 244 la designación de la presidencia.

VIII. PETITORIO:

Por lo expuesto solicito:

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

2- Se declare la admisibilidad del amicus curae.

PROVEER DE CONFORMIDAD

SERÁ JUSTICIA

17 https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

Poder Judicial
Ciudad de Buenos Aires

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

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

Número de CAUSA: EXP 182908/2020-0

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

Escrito: SE PRESENTAN COMO AMICUS CURIAE

Con los siguientes adjuntos:
documental fundacion via libre.pdf

FIRMADO ELECTRONICAMENTE 14/10/2021 07:53:48

MARINARO MARIA SOLEDAD - CUIL 27-23004423-1