SE PRESENTAN EN CALIDAD DE AMICUS CURIAE

Sr juez:

**** abogada, inscripta al TOMO *** FOLIO *** del C.P.A.C.F constituyendo domicilio procesal en ***** de la Ciudad Autónoma de Buenos Aires y domicilio electrónico en ****, en carácter de letrada patrocinante de: ***** (DNI ***), ***** (DNI ****), *** (DNI ****) y *** (DNI ***), 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, nos presentamos y respetuosamente decimos :

I. OBJETO

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

II. LEGITIMACIÓN

2. Somos distintos profesionales de informática, docentes, académicos y personas que participamos en organizaciones de la sociedad civil abogando hace más de 5 años por la autonomía de las personas en relación a las imposiciones y control de las tecnologías sobre nuestros cuerpos, nos

encontramos en calidad y autoridad de expresar a su señoría los riesgos que conlleva el uso generalizado de cámaras de reconocimiento facial.

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 tenga un interés que trascienda al de las partes y se proyecte sobre la comunidad o ciertos sectores o grupos de ella, a fin de resguardar el más amplio debate como garantía esencial del sistema republicano democrático, debe imperar un principio hermenéutico amplio y de apertura frente a instituciones, figuras o metodologías que, por su naturaleza, responden al objetivo de afianzar la justicia entronizado por el Preámbulo de la Constitución"
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.

7. En esta presente causa el cual 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. Se sostiene en dicho amparo 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, violan derechos humanos, asi como nuestra CN y tratados internacionales.
9. En la misma demanda se solicita una medida cautelar de no innovar. Asimismo y como medida cautelar, establecida en el art. 15 de 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. El sistema de reconocimiento facial es una aplicación que identifica automáticamente a una persona mediante un análisis de las características faciales del sujeto extraídas de cámaras de vídeo y comparándolas con una base de datos en la que los sujetos ya están identificados. Toda aplicación de reconocimiento facial está basada en tecnologías de aprendizaje automático, comúnmente denominado machine learning. Los algoritmos de reconocimiento facial deben ser entrenados con bases de datos en donde

aprenden cómo reconocer a las personas de acuerdo a sus rasgos faciales. Estas bases de datos utilizadas para entrenar los algoritmos determinan directamente el tipo de características que se consideran relevantes para identificar un rostro. Es decir, si se utilizan solamente videos o fotos de personas de una etnia, género o edad en particular, el algoritmo se especializa en reconocer esos casos específicos pero no reconoce otros tipos de personas.

V. REPRESENTATIVIDAD DE MINORÍAS POBLACIONALES EN RIESGO.

11. Hay evidencia de público conocimiento[1][2][3] que demuestra cómo la implementación de las cámaras de reconocimiento facial puede atentar contra las poblaciones menos representadas de la sociedad.
12. Si las bases de datos utilizadas para entrenar al sistema no son curadas desde una perspectiva de representatividad social que incluya las personas pertenecientes a etnias o características minoritarias, el sistema entonces tendrá pocos ejemplos de donde aprender para reconocer las adecuadamente. Incluso habiendo cuidado estos aspectos el sistema de reconocimiento facial, por su naturaleza de aprendizaje y generalización inductiva, tendrá invariablemente distintos márgenes de error por lo que se deben tomar decisiones humanas de calibración (por ejemplo aceptar mayor tasa de errores con determinado segmento poblacional, o priorizar falsos negativos por sobre falsos positivos, etc.).
13. En el caso de nuestro país, comúnmente referenciado como “un crisol de razas”, es necesario un peritaje público de que los modelos estén adaptados a las características de las poblaciones que habitan el estado, y que no se atente contra poblaciones menos representadas.
14. En este sentido el estado debe disponibilizar públicamente el set de datos que se ha

[1] Leavy, S. (2018, May). Gender bias in artificial intelligence: The need for diversity and gender theory in machine learning. In Proceedings of the 1st international workshop on gender equality in software engineering (pp. 14-16).

[2] Najibi, A. (2020). Racial discrimination in face recognition technology. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition- technology/

[3] Castelvecchi, D. (2020). Is facial recognition too biased to be let loose?. Nature, 587(7834), 347-349. https://www.nature.com/articles/d41586-020-03186-4

utilizado para crear estos modelos, las decisiones técnicas en la elaboración del modelo, y la transparencia del mismo.

15. DERECHOS SOBRE LOS DATOS PERSONALES

16. La búsqueda de prófugos de la justicia no habilita al estado a avanzar sobre los derechos individuales en términos de privacidad, libre asociación y presunta inocencia. La recolección masiva de datos biométricos por parte del estado sin el consentimiento previo de parte de las personas entra en contravención con la Ley 25.326 de datos personales. En la misma se expresa claramente la necesidad de informar previamente a los titulares de los datos en forma expresa y clara la finalidad para la que serán tratados los datos (biométricos), y dar la posibilidad de ejercer los derechos de acceso, rectificación y supresión de los mismos. La obtención de datos y metadatos individuales, tales como características físicas, sin autorización por parte de los individuos, se ubica como una práctica por fuera del estado de derecho, en el que se presupone que todos los individuos deben ser examinados para comprobar su inocencia.

17. VULNERABILIDADES INFORMÁTICAS

18. Cabe resaltar que todo sistema informático es vulnerable, producto de fallas de software o uso de protocolos informáticos inadecuados para el manejo de datos. Es por esto que ademas de exponer el código del sistema para poder ser auditado, es deber del estado informar cómo y dónde se guardan los datos, qué mecanismos de seguridad hay para limitar quienes acceden a ellos, qué registros hay de tales accesos, y cómo hacen para que esos datos no se utilicen para otros fines.
19. En la misma cuna de la industria informática (San Francisco, EEUU) se ha prohibido su utilización debido a los riesgos que estas conllevan, en tanto manipulación, errores en la identificación, sesgos con minorías y privacidad de los datos. [4]

---

[4] The New York Times (2019). San Francisco Bans Facial Recognition Technology. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

VI. CONCLUSIÓN

20. Teniendo entonces interés legítimo al respecto en virtud de que :
21. 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. [5]
22. El peligro implícito en la utilización de esta tecnología supera con creces las ventajas que la misma pretende brindar a la sociedad.

VII. <u>PETITORIO:</u>

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.

SERA JUSTICIA.

[5] 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.