O.D.I.A.

MANIFIESTA

Sr. juez:

OTERO Matías Daniel, D.N.I. N.º 34.098.950; en mi carácter de apoderado del Observatorio de Derecho Informático, con el patrocinio letrado del **Dr. Rodrigo Sebastián Iglesias**, Abogado, inscripto en el T° 123, F° 621 del C.A.P.C.F., con domicilio electrónico CUIT 20-29392827-5, manteniendo el domicilio constituido, en autos caratulados ***"OBSERVATORIO DE DERECHO INFORMATICO ARGENTINO O.D.I.A. Y OTROS CONTRA GCBA SOBRE AMPARO – OTROS"***, expediente n.° **182908/2020-0**, CUIJ **EXP J-01-00409611-4/2020-0**, a V.S. respetuosamente digo:

I. Objeto

Por medio de la presente vengo, en mi carácter de apoderado del Observatorio de Derecho Informático Argentino, a expresar consideraciones respecto de la tecnología de reconocimiento facial implementada por la demandada, a fin de que sean tenidas en cuenta por el Tribunal al momento de resolver tanto la medida cautelar como el objeto de fondo debatido en las presentes actuaciones.

II. Manifiesta

Sin perjuicio de las medidas probatorias ordenadas en la actuación n° 2384543/2021 del pasado 27 de octubre –las cuales consideramos de pertinencia–, y teniendo en cuenta algunas de las manifestaciones vertidas tanto en la presentación de la demandada (actuación n° 2306959/2021) como en el dictamen de la Sra. Fiscal (actuación n° 2363828/2021), esta parte –cuyo objeto de estudio y análisis de derechos constitucionales en entornos digitales–

entiende de utilidad precisar diversas cuestiones, a fin de intentar aportar claridad y que sean tenidas en cuenta por el Tribunal al momento de resolver la medida cautelar y, posteriormente, la cuestión de fondo.

a. Opacidad

En este sentido, **en primer lugar,** consideramos que no debe perderse de vista lo referido a **la opacidad del funcionamiento del sistema**. La opacidad es un término acuñado dentro del ámbito del derecho informático y que se utiliza para designar sistemas de los cuales se sabe poco o nada respecto de su funcionamiento. De hecho, para una autora como Cathy O'Neil, es uno de los tres presupuestos necesarios para configurar lo que ella llama un *"arma de destrucción matemática"*[1]. Existen dos motivos por lo cual se da la opacidad. Por un lado estos "algoritmos" complejos usan inteligencia artificial, o aprendizaje automático, con lo que no es que una persona escribe paso a paso como resolver un problema, sino que se le da información a la computadora para que encuentre los patrones y haga inferencias sobre ellos. El resultado de este procedimiento es un programa que resuelve un problema, pero ni el creador del mismo sabe cómo lo hace. Por este motivo se les denomina "caja negra", ya que se les da valores de entrada conocidos y de salida esperados y el procesamiento es desconocido. La otra gran barrera para acceder al corazón del sistema y entender su funcionamiento son -generalmente- los derechos de propiedad intelectual. Los software han sido protegidos con el mismo status que los derechos de autor, lo cual implica que su creador posee un poderoso abanico de derechos tanto morales como patrimoniales, entre los que se encuentra la facultad de publicar la obra. En el caso de los programas informáticos la obra es el llamado código fuente, es decir, el conjunto del texto redactado por un experto en un lenguaje específico de programación. Ahora bien, para que la computadora pueda ejecutar ese texto es necesario que a través de otra tecnología

1 Cathy O'Neil, 'Armas de destrucción matemática', Editor digital: orhi, 2016.

se convierta ese texto al sistema binario de ceros y unos. El resultado de esta transformación es ininteligible para los humanos.

Ahora bien, ¿Cómo es posible que muchas empresas distribuyan sus creaciones a los usuarios sin brindar el código fuente ni el conjunto de datos usados para el aprendizaje? Simplemente, entregan una versión ejecutable del mismo (código objeto y redes neuronales entrenadas) y los usuarios aceptan una licencia de uso con grandes restricciones de sus derechos como usuarios.

Tal como sostiene la autora citada anteriormente *"un gran número de empresas se toman muchas molestias por ocultar los resultados de sus modelos o incluso su existencia. Una justificación común es que el algoritmo es un «secreto industrial» crucial para su actividad. Afirman que es propiedad intelectual y la defenderán con legiones de abogados y grupos de presión si es necesario. En el caso de los gigantes web como Google, Amazon y Facebook, solo sus algoritmos hechos meticulosamente a medida valen cientos de miles de millones de dólares"*[2].

En el caso de Facebook, Amazon o Google, los usuarios pueden optar o no por aceptar los términos y condiciones de la licencia de uso y de no hacerlo, simplemente no sufren ninguna otra consecuencia más allá de no poder utilizar el servicio.

Sin embargo, en el caso del sistema de reconocimiento facial de prófugos implementado por el GCBA, la recolección de datos sensibles dispuesta por la autoridad administrativa carece del consentimiento de los ciudadanos que transitan frente a las cámaras de vigilancia. De tal modo, la utilización del sistema aquí impugnado debe necesariamente resultar uno dotado de los niveles de transparencia que rigen la actividad pública. Esto se pone de resalto más aún al tomar en cuenta el carácter crítico de esta tecnología y su innegable vinculación con el ejercicio del ius puniendi en manos de la Autoridad.

---

2 Cathy O'Neil, Op. Cit., pág. 26.

Por otra parte, la propia demandada ha reconocido en la contestación al pedido de información pública efectuado por O.D.I.A., en el cual se le solicitó que se entregara una copia del código fuente del sistema, que *"No se tiene acceso a esta información, por corresponder al secreto comercial de la empresa, que posee el copyright de la licencia del mismo"*. De la atenta lectura de esta respuesta se puede interpretar lo siguiente:

· El Gobierno de la Ciudad de Buenos Aires adquirió solamente una versión ejecutable del sistema.

· No dispone código fuente ni tuvo acceso a los datos usados para su aprendizaje y, por ende, no tiene la capacidad de saber cómo fue diseñado el sistema.

· Aun en el supuesto de que el sistema funcione de manera perfecta conforme a los fines para los que fue diseñado –cosa que como ha sido ya explicada en la demanda y en las demás presentaciones de las partes y amicus curiae, no es posible-, no puede saberse con certeza si se utilizan los datos para otros fines.

El estado al elegir ejercer alguna de las competencias que le son propias mediante el uso de tecnología no puede soslayar la cuestión de la publicidad de los códigos fuente. Debemos recordar que un software es un conjunto de instrucciones para que los ordenadores desarrollen una función. Si esta función es una prerrogativa pública, **la falta de publicidad del código fuente puede equipararse a la falta de publicidad de las normas que rigen el actuar de la administración**. En este caso, no solo el código fuente no está disponible para la población (afectando gravemente el derecho al acceso a la información pública), sino que la administración tampoco tiene acceso al mismo, por lo cual la suerte de los datos de las personas se encuentra en manos de particulares, careciendo el estado de la posibilidad de tener certeza sobre su actuar. Ello importa una especie de privatización de la función pública sin tener el estado la posibilidad de control.

En este mismo sentido, cabe señalar que el mismo GCBA incurre en una desconcertante falacia argumentativa al reconocer que no posee el código fuente ni sabe de qué manera fue entrenado el sistema de reconocimiento y afirmar al mismo tiempo, que el sistema funciona de manera correcta y no produce discriminación alguna. En su contestación de demanda, el GCBA aduce categóricamente que *"El sistema identifica los datos biométricos y no simples parecidos, no habiendo umbral de error de identificación"*, pero sostiene también que *"En relación a los patrones de identificación que hacen al funcionamiento del sistema, sobre los que el amparista formula diversas conjeturas,* ***se hace saber que corresponde al código fuente, sobre el cual el GCABA no es dueño, y el desarrollador no revela****"*. Luego agrega que *"El objeto de la contratación es de la licencia para un servicio, no la adquisición del software. Incluye 300 licencias de uso, de uso simultáneo y rotativo, incluyendo la arquitectura técnica, mantenimiento preventivo y correctivo del software y la arquitectura técnica asociada. Al no ser el propietario de la solución informática,* ***el GCABA no tiene acceso a los recursos que se vieron involucrados en su programación****.* ***Actualmente el sistema no está en proceso de aprendizaje****.* ***Ya recibió su entrenamiento inicial, y solamente contrasta la información que viene del CONARC, con el dato biométrico de los prófugos contenidas en dicha base de datos, extraídos de RENAPER.*** *Cabe aclarar que* ***el sistema utiliza como base de datos primaria la Consulta Nacional de Rebeldías y Capturas****. El sistema no utiliza ni tiene capacidad técnica para identificar los datos biométricos de 45 millones de personas. El sistema* ***no identifica personas que no estén contenidas dentro de esta base de datos de prófugos****. Tiene un limitante técnico.* ***El sistema tampoco está entrenado para identificar determinadas etnias, sino para buscar similitudes****, con 562 puntos de reconocimiento facial. Compara un rostro dado y uno en tiempo real".* (los destacados son propios).

Estos párrafos dan cuenta de que pese a lo sostenido por la demandada, el sistema presenta un alto grado de opacidad, dado que ni siquiera *"el GCBA no tiene acceso a los recursos que se vieron involucrados en su programación".* Dicha circunstancia **implica una grave lesión al derecho de información pública e impide cualquier tipo de control -estatal o ciudadano- sobre el funcionamiento del sistema**. Es importante señalar que la contratación de software puede darse de múltiples maneras actualmente, desde el desarrollo propio hasta la adquisición de licencias de código abierto, por lo que el GCBA no se vio compelido a adquirir una licencia de uso en el modo en que lo hizo, sino que ello fue una elección expresa y deliberada de su parte. Sin embargo, esta elección -la de mayor opacidad posible- restringe drásticamente derechos reconocidos por nuestra Constitución Nacional.

Creemos que este argumento es en sí mismo suficiente para hacer lugar a la pretensión actora. Sin perjuicio de ello, existen más razones que dan cuenta de la opacidad del sistema.

En el acceso al pedido de información pública, la administración no ha dado cabal respuesta a las siguientes preguntas:

a) ¿Qué protocolos de seguridad, privacidad y confidencialidad serán utilizados a efectos de mantener la privacidad de la información recopilada desde su captura hasta su procesamiento?

b) ¿Qué técnica de borrado es utilizada? ¿Cómo se audita y de qué manera se asegura que las imágenes son efectivamente eliminadas?

c) Desde la implementación de este sistema ¿Cuántas imágenes de personas no registradas en el CONARC han sido ingresadas al Sistema de Reconocimiento Facial de Prófugos?

d) ¿A qué requerimiento se refiere la última parte del art. 3 del Anexo de la Resolución 398/19? ¿Por qué este requerimiento tiene que estar dirigido a la Secretaría de Justicia y Seguridad?

e) ¿En qué momentos los agentes destruyen aquellos archivos que le fueron enviados a esos aparatos? ¿Qué sistema o protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos y como se audita su correcta destrucción?

f) ¿A través de qué sistema les llegan las alertas generadas a los Policías? ¿Qué información les son remitidas?

g) ¿Cuántas de las personas detenidas o demoradas, con causa en el levantamiento de una alerta por el Sistema de Reconocimiento Facial, no estaban siendo buscadas por un “delito grave”? Se remite a la definición de “delito grave” utilizada en el anexo de la Resolución 1068 - E/2016.

h) Por el contrario, ¿Cuántas personas han sido detenidas con causa en el levantamiento de una alerta por el Sistema de Reconocimiento Facial de Prófugos, que estaban siendo buscadas por haber cometido un “delito grave”?

i) Para el caso de que la empresa entre en concurso, quiebra o cualquier otra forma reglamentaria de liquidación, o esta sufra algún contratiempo ya sea técnico o administrativo, ¿Se ha previsto algún tipo de control de crisis para proteger los datos de los ciudadanos?

j) ¿Qué método de detección de rostros se utilizó? En caso de utilizar redes neuronales, ¿qué modelo/arquitectura se utilizó y cuál fue el set de datos que se utilizó para entrenar el modelo?

k) **¿Qué datasets fueron utilizados para ese entrenamiento?** (Se ha expresado anteriormente la importancia de saber como fue entrenado el sistema)

l) ¿Se ha hecho una auditoría del software por un tercero independiente;

m) En relación con diversas cuestiones que figuran en el pliego de contratación: a. ¿Qué se quiso decir con “detección de diferentes patrones de comportamiento”? b. ¿Qué se quiso decir con “cambios de condiciones ambientales”? c. ¿Cuál es la cantidad de cámaras instaladas en la vía pública pertenecientes al gobierno de la Ciudad Autónoma de buenos Aires y de la Policía de la Ciudad? d. ¿Qué cantidad de esas cámaras permiten utilizar el software de reconocimiento facial? e. ¿Qué tipo de encriptación se utiliza para el almacenamiento de esas imágenes que generen alertas? f. ¿En qué consisten esos “futuros análisis” que se mencionan? g. ¿Durante cuánto tiempo se guardarán dichas imágenes? h. ¿Dónde se encuentran físicamente los servidores donde se almacena la información del registro resultante entre la inclusión de la base de datos de la CONARC con la del RENAPER, y la información de la estructura facial del rostro capturado por las cámaras instaladas en la vía pública de la Ciudad? i. ¿Qué protocolos de seguridad son utilizados para el almacenamiento de la información del registro resultante entre la base de datos de la CONARC y el RENAPER, y lo grabado por las cámaras instaladas en la vía pública de la Ciudad? j. ¿Quién realiza esta llamada “lista negra”? k. ¿Como y que procedimiento se utiliza para la confección de la llamada “lista negra”? l. ¿Cuántas personas hay en esta lista? m. ¿Cuál es el criterio que se sigue para ingresar y/o egresar de esta lista? 14 n. ¿Quién tiene permiso para modificar esta lista? ¿Qué parámetros o requisitos pide el sistema a efectos de modificar la lista?

n) También en relación con cuestiones relativas al pliego de contratación: a. ¿Qué se considera como un “evento repetitivo” y qué criterios se utilizan para definirlo? b. ¿En qué consiste un “Área de Enmascaramiento” y como puede su consideración evitar “falsos positivos”? c. ¿A qué se refiere con “zonas de detección”? ¿Cuáles son estas zonas? d. ¿A qué se refiere con historia de los eventos? ¿Qué información se almacena? ¿Dónde es almacenada esta información? ¿Quién tiene acceso a esa información y por cuánto tiempo? e. ¿Qué información se considera como “purgable”? ¿Dónde

se almacena esa información? ¿Cuáles son los plazos máximos y mínimos que se consideran a efectos de realizar esa purga? f. ¿Cuántos usuarios con los dos distintos permisos existen? ¿Qué cantidad de usuarios están limitados a la visualización de los datos? ¿Cuántos usuarios existen con total disponibilidad para todas las operaciones? ¿Quién otorga estos permisos? ¿De qué manera y con qué criterio se otorgan esos permisos? 16 g. ¿Cuáles son la totalidad de las operaciones? h. ¿Qué criterio se utilizó a efectos de considerar que un 15% de falsos positivos era un porcentaje aceptable? i. ¿Quién determina las líneas virtuales mencionadas, y dónde se encuentran dichas líneas? j. ¿A qué se refiere con “zona estéril”? k. ¿Cuál es la cantidad (mínima) de personas y durante cuánto tiempo (mínimo) es necesario para que este se considere como hacinamiento? l. ¿En qué condiciones puede suceder un cruce de línea que implique un “acercamiento entre personas”? ¿Cuál es la utilidad práctica de esta categoría? m. ¿Cuánta es la cantidad mínima de personas necesarias para que se dé un caso de “merodeo”? n. ¿Qué se considera como “comportándose de una manera sospechosa”? ¿Cuáles son las actividades puntuales que el sistema está entrenado para reconocer? ¿Cómo se puede prever una actividad delictiva cuando se da este supuesto? o. ¿En qué consiste el presupuesto de “ocupación”? ¿Cuántas personas se necesitan como mínimo en un área para que se configure la ocupación? ¿Cuáles son los presupuestos fácticos de forma detallada para que se configure la ocupación? ¿Cuáles son aquellas áreas pasibles de ocupación? p. ¿En qué consiste la “tolerancia a los falsos positivos” mencionada? 17 q. ¿Con que fin se recolecta la información acerca de la detección de emoción en el rostro de las personas? ¿Por qué se necesita detectar la emoción del rostro de las personas cuando el sistema sería utilizado exclusivamente para la detección de prófugos? r. ¿En qué consiste la indexación mencionada? ¿Qué se considera como “persona de interés? ¿Por qué razón se necesitaría registrar aquella información de estas “personas de interés”?.

Todo ello, pese a que la cuestión fue judicializada y se ha dictado sentencia favorable a la pretensión actora, posteriormente confirmada por la Sala III de la Cámara de Apelaciones del fuero en los autos ***"OBSERVATORIO DE DERECHO INFORMATICO ARGENTINO O.D.I.A. CONTRA GCBA SOBRE ACCESO A LA INFORMACION (INCLUYE LEY 104 Y AMBIENTAL)"***, expediente nº 9480/2019-0.

Es decir, a la fecha, **el GCBA no ha brindado las precisiones requeridas en ejercicio del derecho a la información pública**, **dotando de mayor opacidad al funcionamiento del sistema de reconocimiento facial implementado**.

b. Creación de un riesgo. Falta de proporcionalidad.

En **segundo lugar**, creemos que debe considerarse la desproporcionalidad del riesgo creado en relación con la finalidad que persigue el sistema. El objetivo de la implementación del Sistema de Reconocimiento Facial de Prófugos en la Ciudad de Buenos Aires es ayudar a la captura de las aproximadamente 46.600 personas que figuran en la base del CONARC (Consulta Nacional de Rebeldías y Capturas).

Ahora bien, para ello se recolectan los datos biométricos de todas las personas -catalogados como datos sensibles por la ley nº 25.326 (Anexo I)[3]- pudiendo conocer la ubicación exacta en tiempo real de quienes pasen frente a ellas. El resultado **es una poderosa colección de datos**, en tanto **el Gobierno de la Ciudad de Buenos Aires puede saber en todo momento la ubicación de las personas.**

3 AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, RESOL-2019-4-APN-AAIP

Con relación a ello, el GCBA arguye y la Sra. Fiscal considera que el sistema solo funciona contrastando los rostros que identifica mediante las cámaras de seguridad dispuestas por toda la ciudad con la base de datos del CONARC. Sin embargo, lo cierto es que conforme lo explicado en el punto anterior, no es posible tener certeza de ello ni siquiera el mismo GCBA podría-.

Más aún, en este punto cabe preguntarse si tal idea puede llegar a tener la más mínima lógica. ¿De que modo sería posible que el sistema "descarte" o "enmascare" los rostros de aquellas personas no listadas en el CONARC sin previamente hacer una lectura de todos los rostros posados frente a las Cámaras del GCBA?.

Pero aun cuando se comprobara que efectivamente funciona de esa manera, tal sistema constituye un riesgo desproporcionado para la población en relación con los fines que persigue.

El reciente ataque a la base de datos del RENAPER[4]- mediante el cual se tuvo acceso a todos los datos de todos los DNI existentes en la República Argentina- da cuenta de que el Estado en tanto titular de los datos particulares es susceptible de sufrir vulneraciones de gravedad, las cuales tienen consecuencias dañosas directas sobre la población de tardía, insuficiente o imposible reparación posterior. De hecho, la base de datos de RENAPER es la que complementa la base de datos del CONARC, la cual es utilizada por el SRF. Es por ello que, a mayor cantidad y trascendencia de datos, **mayor debe ser el nivel de seguridad y transparencia que el Estado debe tener en su utilización**. Cabe señalar, una vez más, que <u>los particulares no prestan consentimiento alguno para brindar sus datos biométricos y que son obtenidos compulsivamente por la administración</u>.

---

4 De público conocimiento. Vg. ver https://www.lanacion.com.ar/tecnologia/sigue-la-preocupacion-por-la-difusion-online-de-los-datos-de-argentinos-del-registro-nacional-de-las-nid22102021/

De hecho, remitiéndonos a la escasa información brindada en el pedido de información pública realizado por ODIA, en tanto se le preguntó a la administración: *"Una vez que las imágenes llegan al CMU, ¿cómo se cifra dicha información en el disco y en la memoria RAM? De no ser realizado este cifrado, ¿Qué medidas de seguridad, privacidad y confidencialidad son utilizadas para asegurar su control e integridad?",* la administración contestó que *"Se utiliza un cifrado 3 DES".*

Este tipo de cifrado, como es bien conocido dentro del ámbito de la seguridad informática, es fácil de desencriptar y ello se sabe públicamente desde el año 2016[5]. Es decir, el nivel de seguridad que conocemos del sistema no es suficientemente alto pese a la importancia y trascendencia de los datos que se encuentran en juego.

Es en esta consideración es que se entiende que **el riesgo creado por la implementación del sistema de reconocimiento facial de prófugos, -debido a la sensibilidad de los datos que recoge y máxime teniendo en cuenta la opacidad de su actual funcionamiento- es desproporcionado en relación con los fines para los que fue creado**.

De hecho, así lo entendió Joseph Cannataci, en su carácter de Relator Especial de la ONU sobre el derecho a la privacidad en sus *'Observaciones Preliminares del Relator Especial sobre el Derecho a la Privacidad'* en tanto expresó: *"El 25 de abril de 2019, se activó un sistema de reconocimiento facial en 300 cámaras de vigilancia de la ciudad. El sistema está conectado a la CONARC, la base de datos pública de personas buscadas por la justicia, compuesta por 46.000 archivos. Mis preocupaciones con respecto a la CONARC (ver párrafo 11) también son relevantes aquí. Soy consciente de la necesidad de detener a las personas sospechosas de haber cometido delitos y llevarlas ante la justicia,* ***pero no veo la proporcionalidad de instalar una tecnología con graves***

5 ver https://nvd.nist.gov/vuln/detail/CVE-2016-2183

implicaciones para la privacidad para buscar en una lista de 46.000 personas que actualmente incluye a menores y delitos no graves y que no se actualice y compruebe cuidadosamente su exactitud"[6] (el destacado es propio).

Cabe recordar, además, que el Relator encontró graves fallas en la base datos del CONARC, a saber:

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 solo 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.

---

6 Disponible en https://www.senado.gob.ar/bundles/senadomicrositios/pdf/observatorio/relator.pdf

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.

c. Falta de estudio previo de impacto sobre la privacidad y los datos personales

Un requisito previo a la implementación de tecnologías es la evaluación de impacto en la privacidad y en los datos personales. Las leyes actuales en materia de protección de datos personales disponen la realización de esta evaluación de forma previa y obligatoria, a fin de determinar si la actividad que implique el procesamiento de datos personales que se intenta desarrollar se encuentra justificada y determinar cuál es la relación entre el riesgo y los beneficios de su implementación.

La Agencia de Acceso a la Información Pública de Argentina (AAIP) publicó la Guía de Evaluación de Impacto en la Protección Datos. La AAIP reconoce en dicha guía que *“la interceptación de telecomunicaciones, el monitoreo desproporcionado de los espacios públicos a través de sistemas de videovigilancia, la recolección o publicación de datos personales sin el consentimiento de sus titulares, así como el tratamiento automatizado de información a través de algoritmos o inteligencia artificial representan algunos de los problemas que [el derecho a la protección de datos personales] intenta resolver y de los que se ocupa activamente esta rama del derecho”*. Agrega a continuación

que *“observando con preocupación estos fenómenos de las décadas recientes y con el fin de mitigar los riesgos que entrañan, las Autoridades de Control de la República Oriental del Uruguay y de la República Argentina han decidido cooperar para diseñar un mecanismo de carácter preventivo que busca minimizar los potenciales daños a la privacidad: la Evaluación de Impacto en la Protección de Datos (EIPD)”* y que *“el objetivo de esta herramienta [haciendo referencia a la guía] es que, desde una etapa temprana, las prácticas y proyectos que puedan afectar los derechos de las personas, a través del tratamiento de sus datos personales, sean evaluados por los responsables de tratamiento y constituidos conforme a ciertos estándares restrictivos de seguridad y de integridad”*. Esta normativa tiene como antecedente el Convenio nº 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personales -tratado internacional que tanto Argentina como Uruguay han suscrito y ratificado.

Este estudio no ha sido realizado por el GCBA incumpliendo normativa internacional y nacional.

En conclusión, consideramos que las cuestiones de la opacidad del sistema y el riesgo que implica para la protección de los datos personales y la privacidad de las personas deben ser tenidas en cuenta a la hora de resolver la petición cautelar y de fondo en las presentes actuaciones. No obstante, estas consideraciones deben estar integradas con el conjunto de argumentos brindados por las partes y amicus curiae en el presente proceso. Por último, cabe recordar que, conforme lo considera la Corte Suprema de Justicia de la Nación, *“una moderna concepción del proceso exige poner el acento en el valor “eficacia” de la función jurisdiccional y en el carácter instrumental de las normas procesales, en el sentido de que su finalidad radica en hacer efectivos los derechos sustanciales cuya protección se requiere, y en ese marco de actuación las medidas de la naturaleza de la solicitada se presentan como una de las vías aptas, durante el trámite del juicio, para asegurar el adecuado*

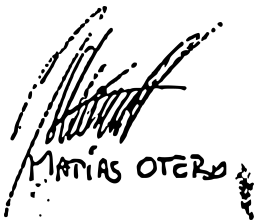
servicio de justicia y evitar el riesgo de una sentencia favorable pero ineficaz por tardía" (CSJN 334:1691).

III. Petitorio.

Se tenga presente lo manifestado al momento de resolver la medida cautelar y la cuestión de fondo debatida en autos.

PROVEER DE CONFORMIDAD

SERA JUSTICIA



Poder Judicial
Ciudad de Buenos Aires

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

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

Número de CAUSA: EXP 182908/2020-0

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

Escrito: MANIFIESTA

FIRMADO ELECTRONICAMENTE 08/11/2021 08:38:23

IGLESIAS RODRIGO SEBASTIAN - CUIL 20-29392827-5