

INICIA AMPARO - MEDIDA CAUTELAR

Señor Juez:

VICTOR ATILA CASTILLEJO ARIAS, abogado inscripto en el T° 133, F° 492 del C.P.A.C.F., representante letrado de **PAULA CASTILLEJO ARIAS**, con DNI N° 19.046.895 con domicilio real en Freire 4439 de esta Ciudad Autónoma de Buenos Aires; y representante letrado de **VICTOR LEOPOLDO CASTILLEJO RIVERO**, con DNI 93.772.464 y domicilio real en Conesa 3997; y constituyendo todos domicilio procesal en Conesa 3997 y procesal electrónico en 20-19054367-7 y correo electrónico en victorcastillejo21@gmail.com, en esta Ciudad Autónoma de Buenos Aires, me presento ante V.S. y digo:

1. OBJETO

Que vengo por instrucciones de mis representados a adherir como partes actoras en el presente litigio en donde se está realizando un control de constitucionalidad y convencionalidad de la Resolución N° 398/MJYSGC/19 y de la Ley N° 6339, en cuanto se implementó el “SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS” (de ahora en más “SRFP”), y se modificó la Ley N° 5688 artículos 478, 480, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis, por ser contraria a los artículos n° 14, 14bis, 18, 19, 33, 43, 75 inc. 22 de la Constitución Nacional; artículos n° 14, 16, 18, 34, 36, 38, 39, 61 de la Constitución de la Ciudad de Buenos Aires, a la OC 5/85 de la CIDH (Derecho a Reunión de Terceros), al art. 1710 del CCCN, al art. 7 del Pacto de San José de Costa Rica, a los artículos 4, 5, 7, 9, 14, 17, 20, 21, 24 del Pacto de Derechos Civiles y Políticos, y a las leyes N° 2145 de la Ciudad Autónoma de Buenos Aires, n° 1845 de CABA sobre protección de datos personales y N° 25.326 de Protección de Datos Personales.

2. LEGITIMIDAD ACTIVA

La Constitución Nacional sancionada en 1994, en su nuevo artículo 43 establece que toda persona puede interponer acción expedita y rápida de amparo contra todo acto u omisión de autoridades públicas que, en forma actual o inminente, lesione, restrinja, altere o amenace con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por la misma.

En el mismo sentido, la Constitución de la Ciudad de Buenos Aires, agrega: “[...]

Están legitimados para interponerla cualquier habitante y las personas jurídicas defensoras de derechos o intereses colectivos, cuando la acción se ejerza contra alguna forma de discriminación, o en los casos en que se vean afectados derechos o intereses colectivos, como la protección del ambiente, del trabajo y la seguridad social, del patrimonio cultural e histórico de la Ciudad, de la competencia, del usuario o del consumidor. [...]” (el destacado es propio).

En este sentido, al ser ambos actores ciudadanos y residentes de esta Ciudad Autónoma de Buenos Aires, que transitan en su vida diaria a través de sus calles, la implementación de este SRFP implica una injerencia -en sus derechos a la privacidad, intimidad y protección de los datos personales, entre otros- totalmente intolerable en un estado de derecho. Adicionalmente, la implementación de este SRFP representa un riesgo de detención inminente, lo cual atenta contra su derecho a la libertad ambulatoria y presunción de inocencia en virtud de que el SRFP utilizado es sumamente ineficiente lo que podría llevar a detenciones arbitrarias conforme se demostrará más adelante.

3. ADMISIBILIDAD DE LA ACCIÓN

Por el otro lado, la Ley de Amparo de la Ciudad Autónoma de Buenos Aires N° 2145 exige, en esencia, los siguientes requisitos para su procedencia: a) Que no exista otro medio judicial más idóneo; b) Que se interponga contra un acto u omisión de alguna autoridad pública o de algún particular; c) Que en forma actual o inminente se lesione, restrinja, altere o amenace con arbitrariedad e ilegalidad manifiesta, derechos y garantías previstos en el plexo normativo de la ciudad; y d) Que el amparo se interponga dentro de los 45 días hábiles contados a partir de que el afectado hubiese obtenido conocimiento cierto de la lesión, restricción, alteración o amenaza.

Como notará V.S. todos esos supuestos se encuentran cumplidos en el presente.

a) Medio judicial más idóneo.

En primer lugar, el Amparo es el medio judicial más idóneo por que las circunstancias en las cuales se han dado los hechos relacionados a este proceso así lo determinan. La Resolución 398 y la Ley 5688 restringen y alteran con absoluta arbitrariedad manifiesta, derechos y garantías reconocidos por la Constitución Nacional y de la Ciudad; en particular los artículos 14, 14 bis, 18, 28 y 31 de la Constitución Nacional, lesionando los derechos de ejercer de reunión y asociación, libertad

ambulatoria, igualdad, privacidad, principio de inocencia, debido proceso, autodeterminación informativa, entre otros, con arbitrariedad, incongruencia e irrazonabilidad manifiesta, conculcando derechos y garantías reconocidos por la Constitución Nacional. En virtud de ello el pronunciamiento de su inconstitucionalidad no puede esperar y la acción expedita de amparo es el único medio mediante el cual se pueden proteger estos derechos.

Actualmente se encuentra tramitando ante el Tribunal Superior de Justicia de esta Ciudad Autónoma de Buenos Aires una “*Asociación por los Derechos Civiles c/GCBA s/acción declarativa de inconstitucionalidad*” (Expte. N° 17642/19). En este expediente tramita una acción declarativa de inconstitucionalidad en conforme el art. 113, Inc. 2° de la CCABA y Art. 17 de la Ley 402 contra la Resolución 398 planteada por la Asociación por los Derechos Civiles (de ahora en más “ADC”). No obstante, la inconstitucionalidad que aquí solicitamos radica en la lesión de derechos y principios distintos que los alegados en aquella acción declarativa y, como veremos, se han descubierto hechos nuevos que demuestran con claridad lo profundamente lesivo e inconstitucional que la implementación de la Resolución 398 y la Ley 5688, en sus artículos 478, 480, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis, han tenido en los derechos de mis representados que son ciudadanos de la C.A.B.A y transitan por sus calles de manera habitual.

b) Se interponga contra un acto u omisión de alguna autoridad pública.

Esta acción se presenta contra la Resolución 398 del MJYSGC y la ley 5688 que implementó el Sistema de Reconocimiento Facial de Prófugos. Por lo tanto, este requisito se encuentra cumplido.

c) Lesión, restricción, alteración o amenaza, con arbitrariedad e ilegalidad manifiesta, de derechos y garantías.

Si bien este punto lo profundizaremos más adelante, existen una variedad de derechos importantes, y que hacen a la piedra fundamental de cualquier sociedad democrática, que han sido lesionados, restringidos y alterados. No obstante, en este apartado mencionaremos los que a nuestro criterio son algunos de los más importante.

Para empezar, la implementación de este sistema elimina de manera absoluta el principio de presunción de inocencia. Esto así por que cualquier alerta que se derive del

uso de este sistema habilita la intervención de la policía la cual te puede detener de manera intempestiva y pesa sobre aquella persona que ha levantado una alerta una presunción de culpabilidad intolerable en un estado de derecho. Ejemplos son muchos, pero uno de los principales es el caso del Sr. Guillermo Ibarrola que fue detenido por 6 días a causa de una alerta de este sistema, habiéndoselo culpado de un delito que él nunca había cometido¹.

En segundo lugar, surge del pliego de contratación directa inicial mediante el cual se adquirió este Sistema de Reconocimiento Facial, que el sistema debía alertar cuando ocurrieran eventos que tienen una amplitud realmente impresionante. Por ejemplo, se exigía en dicho pliego que el sistema pudiera reconocer que alguien se estuviera “comportándose de manera sospechosa” sin siquiera determinar que se quiso decir con esa expresión. Así también se solicitaba que se pudieran detectar “patrones de comportamiento” y la posibilidad de detectar “hacinamiento”, fórmula detectada para el levantamiento de una “alerta por la detección de una cierta cantidad de personas detectadas durante una cierta cantidad de tiempo”. Este tipo de expresiones abiertas son sumamente perjudiciales para los derechos de mis representados ya que alteran gravemente derechos de raigambre constitucional tales como el derecho a la libre reunión y asociación, derecho a la huelga, entre otros.

En tercer lugar, la información obtenida a través de estos datos no son objeto de un tratamiento de datos adecuado y la información que se obtiene de esas cámaras es resguardada con protocolos de encriptación muy bajos que ponen en peligro los datos personales, la privacidad y la autodeterminación informativa de mis representados que pasan por estas cámaras.

Así también, la ciudadanía -incluyendo a mis representados- ha sido directamente engañada en cuanto se le ha prometido que dicho SRFP posee una efectividad en el reconocimiento de las caras que, por información proveniente del propio estado, este sistema NO POSEE. Es decir, que la efectividad del sistema no es del 96%, 92% o 100% conforme lo han repetido reiteradas veces desde el GCBA².

¹ Ver <https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-presos-por-un-error-del-sistema-de-reconocimiento-facial/>

² Ver <https://www.infobae.com/sociedad/policiales/2019/04/24/reconocimiento-facial-en-la-ciudad-de-buenos-aires-como-sera-el-sistema-que-ayudara-a-capturar-a-los-46-mil-profugos-de-la-justicia/> ;

No obstante la enunciación de estos claros supuestos, a lo largo de esta presentación se realizará una evaluación pormenorizada de los derechos y garantías lesionados y de la ilegalidad manifiesta que la implementación de este SRFP representa.

d) Plazo de interposición de la acción

Señalamos que en el antecedente “Gil Domínguez, Andrés c/ GCBA s/ acción declarativa de inconstitucionalidad” Expte. n° 5296 este plazo de 45 días ha sido declarado inconstitucional por el Tribunal Superior de Justicia. No obstante, esta parte se ha enterado de la existencia de este proceso mediante la publicación de los edictos que establecieron un plazo de 15 días para que se presente todo aquel que entienda que tiene un interés jurídico en el litigio a presentarse como parte.

4. ARGUMENTOS FÁCTICOS Y JURÍDICOS

A. El SRFP no es eficiente.

Uno de los fundamentos más relevantes para haber sostenido la implementación del S.R.F.P. ha sido su presunta eficiencia en el reconocimiento de las caras de los individuos que formarían parte del CONARC y que supuestamente se encontraría “prófugos de la justicia”.

A título meramente ejemplificativo, la Jefa de Gabinete de la Secretaría de Administración de Seguridad del GCBA ha dicho³:

<https://www.lavoz.com.ar/sucesos/cayeron-7-profugos-detectados-con-nuevo-sistema-de-reconocimiento-facial>

³ Ver <https://www.infobae.com/sociedad/policiales/2019/04/24/reconocimiento-facial-en-la-ciudad-de-buenos-aires-como-sera-el-sistema-que-ayudara-a-capturar-a-los-46-mil-profugos-de-la-justicia/>

Mediante el reconocimiento facial se generarán alertas de detención de personas buscadas exclusivamente por orden judicial. "El porcentual de acertividad es de 93% en el total de pruebas que se realizaron. Es uno de los mejores reconocimientos faciales de prófugos del mundo, en los máximos estándares internacionales", explicó Cecilia Amigo, jefa de gabinete de la secretaría de Administración de Seguridad.



El sistema fue presentado por Diego Santilli junto a Raquel Casanelli (comisario de la Policía de la Ciudad), Cecilia Amigo, jefa de gabinete de la secretaría de Administración de Seguridad y Anibal Fajrrena, subsecretario de Investigaciones y Estadística Criminal

Asimismo, el Vicejefe de Gobierno porteño Diego Santilli ha dicho que este sistema tiene una efectividad perfecta⁴:

⁴ Ver <http://notasdeactualidad.com.ar/santilli-destaco-la-efectividad-del-sistema-de-reconocimiento-facial/>

El vicesecretario de gobierno porteño indicó que "hay más de cuarenta mil personas en situación de pedido de captura y que la justicia pide que se presenten". En las primeras 48 horas del mecanismo cayeron varios prófugos.



El jueves pasado por la mañana comenzó a utilizarse el nuevo Sistema de Reconocimiento Facial que presentó el gobierno de la ciudad de Buenos Aires. Durante el primer día, siete prófugos de la Justicia lograron ser identificados y detenidos, mientras que en las últimas horas se sumó el caso más emblemático: un hombre de 50 años acusado por violación que era buscado desde 2017.

En ese marco, el vicesecretario de Gobierno porteño Diego Santilli aportó más detalles de este mecanismo, al cual calificó como "100% efectivo hasta el momento". "Con el plantel de 7 mil cámaras, es diferente al lector de patentes porque esto sólo opera con la base de datos de personas prófugas. Es una base de datos pública del Ministerio de Justicia de la Nación, donde todas las provincias van integrando allí todas las personas buscadas", señaló el funcionario en diálogo con Sábado Tempranísimo por Radio Mitre.

En adición, el mismo MJySGC al contestar las preguntas realizadas por la ONG ODIA -que consta en los documentos acompañados por ella como prueba- (NO-2019-33745359-GCABA-DGEYTI o Anexo I) respondió lo siguiente: "60) *¿Qué compromiso tuvo la empresa respecto a la cantidad posible de falsos positivos que su sistema podía generar?*" a lo que se respondió "Se ratifica lo informado oportunamente, en cuanto a que el índice de precisión es superior al 95% conforme a lo enunciado en el pliego técnico del oferente." (el destacado y subrayado es propio)

No obstante estas manifestaciones, con la información que ha sido oportunamente recolectada por ODIA, se descubrió que dicha efectividad alegada es completamente falsa.

Para empezar, en la respuesta brindada a ODIA en fecha 15 de agosto de 2019 mediante la nota NO-2019-25581723-GCABA-DGEYTI (Anexo II), el GCBA respondió a la pregunta 49, "49) *¿Cuántas alertas ha disparado el sistema desde su implementación*

y puesta en funcionamiento?” lo siguiente: “Alertas arrojadas 3059.” (El destacado y subrayado es propio).

Así, con esta respuesta, se descubrió que la cantidad de alertas arrojadas por el sistema hasta la fecha del 15 de agosto de 2019, pero, para poder evaluar verdaderamente su efectividad faltaba que el ministerio contestara cuantas de aquellas personas habían sido verdaderamente puestas a disposición de la justicia.

En el amparo de acceso a la información pública presentado por ODIA (Número de Causa 9480/2019-0) se logró obtener, mediante la nota NO-2019-33745359-GCABA-DGEYTI acompañada como Anexo I de fecha 30 de octubre de 2019 (dos meses y medio después de haber recibido ODIA la respuesta a la pregunta N° 49), la respuesta a la pregunta 50. En dicha pregunta ODIA inquirió “50) *¿Cuántas personas han sido detenidas o demoradas al día de la fecha con causa en el levantamiento de una alerta por el sistema de reconocimiento facial?*”

A esta pregunta, el GCBA respondió: “*El total de personas identificadas puestas a disposición de la Justicia fueron 1.337 hasta el 25 de julio del corriente año. A la actualidad, 1648 personas han sido puestas a disposición de la justicia.*” (el destacado y subrayado es propio).

Esto quiere decir que si al 30 de octubre de 2019 se habrían puesto a disposición de la justicia 1648 personas y sabemos que al 15 de agosto de 2019 las alertas arrojadas habrían sido 3059, podemos hacer una regla aritmética simple para determinar el estimado real de la efectividad del sistema. Para ello, deberemos tomar la cantidad de personas puestas a disposición de la justicia (1648) y averiguar que porcentaje representa del total de alertas arrojadas (3059). Para ello, una regla de tres simple será suficiente:

$$1648/3059 = 0.538738 * 100\% = \underline{\underline{53.5738 \%}}$$

Como no se le escapará a V.S., en este análisis no estamos teniendo en cuenta la diferencia de 2 meses y medio entre las alertas arrojadas en fecha 15 de agosto de 2019 y las posibles alertas realizadas al 30 de octubre de 2019. Estos dos meses y medio faltantes podrían llevar a este número de 53.5738% de efectividad mucho más abajo.

Como puede ver V.S. esto quiere decir que la implementación de este sistema no solo es ilegítimo si no que introduce un elemento que pone en riesgo la libertad ambulatoria a mis representados que son ciudadanos de la Ciudad Autónoma de Buenos Aires.

El Art. 18 de nuestra Constitución Nacional establece, en su parte pertinente, lo siguiente: “*Artículo 18.- [...] Nadie puede ser obligado a declarar contra sí mismo; **ni arrestado sino en virtud de orden escrita de autoridad competente.** Es inviolable la defensa en juicio de la persona y de los derechos. [...]*”.

De la claridad de este presupuesto surge el principio que determina que la policía no puede detener, demorar, o arrestar a un individuo a no ser que exista una orden escrita de autoridad competente. No obstante, las normas prevén excepciones. Una de estas excepciones son las que provienen del art. 5, Inc. 1 del Decreto-Ley 333/58 (modificado por ley 23.950) que determina lo siguiente: “*Artículo 5º.- Son facultades de la Policía Federal para el cumplimiento de sus funciones:*

1.- Fuera de los casos establecidos en el Código de Procedimientos en Materia Penal, no podrá detener a las personas sin orden de juez competente. Sin embargo, si existiesen circunstancias debidamente fundadas que hagan presumir que alguien hubiese cometido o pudiere cometer algún hecho delictivo o contravencional y no acreditase fehacientemente su identidad, podrá ser conducido a la dependencia policial que correspondiese, con noticia al juez con competencia en lo correccional en turno y demorada por el tiempo mínimo necesario para establecer su identidad, el que en ningún caso podrá exceder de diez horas. Se le permitirá comunicarse en forma inmediata con un familiar o persona de su confianza a fin de informarle su situación. Las personas demoradas para su identificación no podrán ser alojadas junto ni en los lugares destinados a los detenidos por delitos o contravenciones. (Inciso sustituido por art. 1º de la Ley N° 23.950 B.O. 11/9/1991)” (el destacado y subrayado es propio).

A mayor abundamiento, la ley de la provincia de Buenos Aires 13.482 en su art. 15 inc. “c” “*Artículo 15: El personal policial está facultado para limitar la libertad de las personas únicamente en los siguientes casos: [...] c) Cuando sea necesario conocer su identidad, en circunstancias que razonablemente lo justifiquen, y se niega a identificarse o no tiene la documentación que la acredita. Tales privaciones de libertad deberán ser notificadas inmediatamente a la autoridad judicial competente y no podrán durar más del tiempo estrictamente necesario, el que no podrá exceder el término de doce (12) horas. Finalizado este plazo, en todo caso la persona detenida deberá ser puesta en libertad y, cuando corresponda, a disposición de la autoridad judicial competente.*” (el destacado y subrayado es propio).

Es decir, esta facultad que tiene la policía de detener a las personas en la calle es una facultad que, en un estado de derecho, debe ser ejercida de manera sumamente restrictiva. Detener a alguien en la calle no es una decisión que deba tomarse a la ligera ya que se estarían violando los derechos constitucionales más íntimos de los individuos como puede ser el derecho a la libertad ambulatoria. En este punto, es necesario destacar las palabras de la Corte Interamericana de Derechos Humanos en cuanto ha dicho que “[...] nadie puede ser sometido a detención o encarcelamiento por causas y métodos que -aun calificados de legales- puedan reputarse como incompatibles con el respeto a los derechos fundamentales del individuo por ser, entre otras cosas, irrazonables, imprevisibles, o faltos de proporcionalidad. [...]”⁵.

Teniendo en cuenta que nuestra parte considera ilegítimo el hecho que se pueda detener a alguien al solo efecto de determinar su identidad, de la propia norme surge que tienen que existir circunstancias “debidamente fundadas” o que “razonablemente lo justifiquen”. Mi parte entiende que una alerta que surja de **este SRF no es una circunstancia de este tipo.**

Sin embargo, el accionar de la policía ante el levantamiento de una de estas alertas es detener al individuo e intentar determinar su identidad. Esto surge con absoluta claridad de la pregunta N° 41 realizada en el pedido de acceso a la información pública de ODIA. En este sentido ODIA habría preguntado lo siguiente: “*El reporte de una alerta del sistema, por si sola, ¿es una circunstancia que justifica la **detención o demora** de una persona?*”. A esto, el GCBA contestó “*Si porque los datos que saltan en la alerta **proviene de la base de datos del CONARC** en el cual se cargan todas las causas en las*

⁵ Caso Gangaram Panday vs. Suriname, del 21-01-94, párr. 47; Caso Chaparro Alvarez y Lapo Iñiguez párr. 90; Caso Neptune, párr. 97.

que las personas tienen pedidos de capturas o se encuentran estado de rebeldía.” (el destacado es propio)

Como puede ver V.S. el mero hecho de que se levante una alerta en este Sistema de Reconocimiento Facial de Prófugos **implica necesariamente que la policía salga a detener al individuo que levantó esa alerta.** Esto es sumamente problemático y palmariamente inconstitucional, ya que, como hemos visto, el SRFP tiene una efectividad que se encuentra por debajo del 50%. Nos debemos preguntar, V.S., ¿cual puede ser la legitimidad de un sistema que introduce en nuestra sociedad un elemento en el cual las personas pueden ser víctimas de detenciones y demoras arbitrarias?

Por más que la mitad de esas personas estén efectivamente en el CONARC, ¿se justifica que se perturbe la vida civil de mis representados que no están en esa lista? Tan es así V.S. que ya existen abundantes casos en los cuales se han detenido personas que fueron detenidas arbitrariamente. Así, por ejemplo, se detuvo a una mujer⁶ que demostró fehacientemente con su Documento Nacional de Identidad que no era la persona que efectivamente la policía se encontraba buscando. Y aún así, la policía se la llevó detenida por un mero “parecido” y permaneció presa por más de 24 horas.

Así también se detuvo a un hombre **por más de 6 días** por el simple hecho de que en el CONARC se había ingresado un DNI distinto al que de verdad estaba imputado⁷. El mismo era acusado por haber cometido un robo agravado en Bahía Blanca. El único detalle es **que el nunca había pasado por Bahía Blanca** y nunca había cometido un delito. Lo más dramático es que un móvil policial ya iba con el ciudadano esposado hacia una prisión en bahía blanca cuando la fiscal del caso advirtió que tenían a la persona equivocada:

⁶ Ver <https://www.pagina12.com.ar/194339-detenido-por-el-parecido-con-una-persona-buscada>

⁷ Ver <https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-presos-por-un-error-del-sistema-de-reconocimiento-facial/>



8

Existen otros casos como el de una mujer que llegaba a Retiro proveniente de la provincia de Mendoza y policías entraron en el vagón de tren para detenerla por una causa sobre la cual ya estaba sobreseída y había sido realizada por una expareja enojada. Para ello la tuvieron arrestada por un rato hasta que finalmente la dejaron libre⁹:



10

V.S. estos casos no son más que solamente aquellos que han tomado estado público y le recomendamos enormemente que acceda a ver los videos que demuestran con una claridad inusitada lo problemático y completamente inconstitucional de este SRFP. El

⁸ <https://www.youtube.com/watch?v=oXM3dQpN9k4> y <https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-presos-por-un-error-del-sistema-de-reconocimiento-facial/>

⁹ Ver el video en https://www.clarin.com/policiales/identificaron-14-personas-dia-reconocimiento-facial-81-quedo-libre_0_O_WhA1FAf.html

¹⁰ <https://www.youtube.com/watch?v=mi91K8SDGbk&t=43s>

único elemento que los junta a todos es que este SRFP no ha funcionado como debería. Se han detectado casos de mal reconocimiento de la cámara, así como un error al ingresar los datos en el CONARC. Independientemente de ello, la efectividad que ha demostrado tener este sistema para encontrar supuestos “prófugos” es realmente paupérrima y ha generado daños palpables a muchas personas de esta Ciudad Autónoma de Buenos Aires. Esto, por supuesto, pone a mis representados en un estado de preocupación totalmente injustificable. ¿llegará el día donde este “Sistema” indique equivocadamente que ellos han cometido un ilícito?

Es realmente sorprendente que en un Estado de Derecho se permita la existencia de este tipo de sistemas ya que no solo no ayudan a reducir el delito sino que introduce un elemento de riesgo para los derechos de sus ciudadanos -entre los que se encuentran mis representados- en las calles de nuestra ciudad. Si mis representados se encontraran transitando por las calles de la CABA, estos pueden ser víctimas de una detención arbitraria de este tipo en absoluta violación a sus derechos a la libertad y a la privacidad. Como sociedad **no podemos permitir que se utilice un sistema que gatilla el poder punitivo del estado por el mero hecho de que una persona se “parezca” a alguien que haya cometido algún delito.**

Este SRFP también afecta al Principio de Presunción de Inocencia. Recordemos que nuestro Art. 18 establece que ninguna persona puede ser penada sin juicio previo fundado en ley anterior al hecho del proceso. Además de nuestra Constitución Nacional esta garantía aparece en el Derecho Internacional y se la puede encontrar en: la Declaración de los Derechos del Hombre y del Ciudadano, en su artículo 9 “[...] *todo hombre se presume inocente mientras no sea declarado culpable* [...]”; en la Declaración Universal de los Derechos Humanos en su artículo 11: “[...] *Toda persona acusada de delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad, conforme a la ley y en juicio público en el que se le hayan asegurado todas las garantías necesarias para su defensa.* [...]”; y finalmente en la Convención Americana sobre Derechos Humanos la cual establece en su artículo 8, segunda parte, que: “[...] *Toda persona inculpada de delito tiene derecho a que se presuma su inocencia mientras no se establezca legalmente su culpabilidad.* [...]”.

Este SRFP lo que hace es precisamente invertir este principio y pone a mis representados en una posición en la cual tienen que brindar explicaciones al Estado de porque no tienen nada que ver con la detención que se está llevando a cabo.

Imagínese V.S. la siguiente historia hipotética. Usted se levanta un día de semana temprano y desayuna con su familia en la seguridad de vuestro hogar. Toma café, quizás alguna medialuna o algún tostado con jugo de naranja -si tiene la suerte de tenerlo en su heladera-. Piensa “hoy va a ser un buen día” y después de saludar cariñosamente a su familia se dirige a su juzgado, quizás con el diario bajo el brazo, en el transporte público. Se toma la línea D del subte por que sabe que se puede bajar en estación Catedral y dirigirse caminando tranquilamente a su oficina que se encuentra a pocas cuadras. No obstante, cuando el subte llega a la estación entran dos policías con mala cara exigiéndole la presentación de documentación que acredite su identidad. Todo esto, por supuesto, con miradas suspicaces provenientes de vecinos que seguramente piensen hacia sus adentros “algo habrá hecho”. Le comentan que usted ha levantado una alerta en este novedoso e inequívocabable Sistema de Reconocimiento Facial de Prófugos y lo acusan de algún robo, hurto o de no haberse presentado en tiempo como testigo en un juicio (¡dios quiera sea solamente eso!). Usted sabe que el funcionario policial está equivocado por que nunca se ha visto involucrado en un juicio, robo o hurto, pero el funcionario está obligado a comunicarse con la fiscalía para ponerlo a usted, que nada tiene que ver con ese asunto, a disposición de alguien que probablemente no lo conozca y no entienda que, sin usted presente en el juzgado, los despachos de ese día no van a ser firmados.

Usted le avisa al funcionario policial esta situación y el mismo le manifiesta que la decisión no pasa por él, pasa por el fiscal o el juzgado que haya ordenado esa orden de captura. Espera pacientemente por horas mientras el oficial policial intenta comunicarse con alguien en la fiscalía. No encuentra a nadie. Usted se enoja (¡con toda la razón!) porque sabe que nada ha hecho. Pero no obstante se ve obligado a sufrir esta injerencia totalmente arbitraria e innecesaria en su vida, donde debe explicarle a alguien que nada tiene que ver con usted, que nada ha hecho. Y acá termina la historia.

V.S., como esta corta historia espero explique de manera sencilla, eso mismo es lo que sucedería casi todos los días en las calles de la ciudad de buenos aires si se siguiera permitiendo la existencia de este sistema probadamente defectuoso y flagrantemente inconstitucional. Historias donde gente de bien se encuentra transitando normalmente cuando interrumpe su buen día un desafortunado funcionario policial solicitándole explicaciones de porque un SRFP defectuoso levantó una alerta con su cara. Esto, por supuesto, de manera absolutamente contraria al principio de presunción de inocencia.

Dicho esto, es necesario ahora ahondar en la razón por la cual se ha buscado implementar este Sistema y si este SRFP realmente logra su objetivo, o, por el contrario, es totalmente desproporcional usar este sistema para “detener prófugos”.

B. Ausencia de razonabilidad y proporcionalidad.

El art. 28 de nuestra C.N. establece “*Artículo 28.- Los principios, garantías y derechos reconocidos en los anteriores artículos, no podrán ser alterados por las leyes que reglamenten su ejercicio.*”. Se podría argumentar que esta disposición deriva directamente de lo que Juan Bautista Alberdi ha sostenido a lo largo de su vida: “*No basta que la Constitución contenga todas las libertades y garantías conocidas. Es necesario... que contenga declaraciones formales de que no se dará ley que, con pretexto de organizar y reglamentar el ejercicio de esas libertades, las anule y falsee con disposiciones reglamentarias. Se puede concebir una constitución que abrace en su sanción todas las libertades imaginables, pero que admitiendo la posibilidad de limitarlas por ley, sugiera ella misma el medio honesto y legal de faltar a todo lo que promete.*”¹¹.

¿Qué es lo que nos quería decir Alberdi?

Básicamente, que de nada sirve tener derechos y garantías en nuestra constitución si después alguno de los poderes del estado, vía actividad reglamentaria o legislativa, afecta o limita de alguna forma ilegítima dichos derechos y garantías.

En este mismo sentido, las palabras de la Dra. Gelli son sumamente elocuentes “*Aunque el art. 28 no contiene la expresión, la doctrina y la jurisprudencia han elaborado el principio de razonabilidad, como un intento de delimitación entre la reglamentación legítima y la que altera los derechos y garantías, tarea compleja y nada sencilla de resolver. No obstante, es posible afinar las pautas a criterios de razonabilidad para delinear un principio interpretativo que afiance los controles y resguarde los derechos.*

El principio interpretativo de razonabilidad, de todos modos, emana de una norma operativa por lo que resulta ineludible de aplicar por todos los órganos de poder en el estado de derecho, entendido éste, precisamente, como estado de razón. En efecto,

¹¹ Las Bases, Editorial Plus Ultra, 1998, Cap. XXXIII. La Constitución debe precaverse contra leyes orgánicas que pretendan destruirla por excepciones. Examen de la Constitución de Bolivia. Modelo del fraude en la libertad.

si lo razonable es lo opuesto a lo arbitrario, es decir contrario a lo carente de sustento -o que deriva sólo de la voluntad de quien produce el acto, aunque esa voluntad sea colectiva-, una ley, reglamento o sentencia son razonables cuando están motivados en los hechos y circunstancias que los impulsaron y fundados en el derecho vigente.”¹² (el destacado y subrayado es propio).

Así también: “*Pero una norma puede cumplimentar los requisitos del debido proceso adjetivo y ser, no obstante, inconstitucional. Ello sucede cuando el contenido de la norma, la sustancia de la disposición, la reglamentación de los derechos o garantías carece de razonabilidad, es decir, afecta o vulnera el debido proceso sustantivo o material.*”¹³

En la misma línea es doctrina de nuestro Tribunal Címero que es la razonabilidad con que se ejercen las facultades discrecionales el principio que otorga validez a los actos de los órganos del Estado y que permite a los jueces, ante planteos concretos de parte interesada, verificar el cumplimiento de dicha exigencia.¹⁴

Así las cosas, es menester preguntarnos, ¿Es razonable la Resolución 398 y la ley 5688 en sus artículos en cuestión mediante los cuales se implementa este Sistema de Reconocimiento Facial? Veamos.

La misma Res. 398 en sus considerando establece lo siguiente: “*Que en tal sentido, se ha desarrollado el Sistema de Reconocimiento Facial de Prófugos, como un instrumento comprendido dentro del Sistema Público de Video Vigilancia de la Ciudad Autónoma de Buenos Aires, el cual **mediante una cámara de video vigilancia reconoce los rostros de las personas requeridas por orden judicial**, registradas en las Bases de Datos del Sistema de Consulta Nacional de Rebeldías y Capturas (CONARC) del Registro de Reincidencia del Ministerio de Justicia y Derechos Humanos de la Nación;*” (el destacado es propio).

Como no se le escapará a V.S., esto quiere decir que para determinar si las caras que una Cámara de Video Vigilancia está grabando están efectivamente en la base de datos del CONARC, la misma tiene que comparar todas las caras que surgen de las imágenes tomadas por la policía. Acá se presenta el primer problema de proporcionalidad y razonabilidad. Esto así, por que al tener que necesariamente tomar las imágenes de todas las personas en la imagen y realizarles un tratamiento para determinar si son o no

¹² GELLI, María Angélica “CONSTITUCIÓN DE LA NACIÓN ARGENTINA. COMENTADA Y CONCORDADA” 3era. Edición Ampliada y Actualizada. Buenos Aires. La Ley, 2006. Pag. 327

¹³ Op. Cit. Pag. 328

¹⁴ “Elias, Jalife s/Acción de Amparo” 16/12/1993. CSJN.

son de personas que se encuentran en aquella base de datos, se está violando el derecho a la privacidad de absolutamente todos los individuos -como mis representados- que pasen por alguna de aquellas cámaras. En este punto, el hecho que posteriormente borren (o no) las imágenes, no es relevante, ya que el hecho dañoso ya está ocurriendo. Es decir, tomar datos personales (de carácter sensible) de los individuos sin haber tomado el consentimiento previo de cada uno de ellos.

La ley de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires dice, en primer lugar, que un “dato personal” es “[...] *Información de cualquier tipo referida a personas físicas o de existencia ideal, determinadas o determinables. [...]*”. Esto quiere decir que podemos concluir sin demasiada controversia que al tomar estas imágenes de los ciudadanos para contrastarlos con una base de datos (o imágenes) existentes, es estar tomando datos personales de los ciudadanos. Sin embargo, estos datos personales son de una categoría que merecen incluso una protección mayor. La ley también dice que serán datos sensibles “[...] *Aquellos datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos. [...]*”. En este sentido, y si bien ahondaremos más adelante en este punto, el tomar las imágenes de las caras de mis representados para contrastarlas con una base de datos implica necesariamente un tratamiento que involucra la discriminación de las mismas. A su vez, estos datos también guardan información propia acerca de la salud y el origen racial o étnico de los individuos, por lo que cada una de las imágenes (y de la información derivada de esas imágenes) son necesariamente un dato sensible. Asimismo, estos datos son de carácter biométrico, lo que los hace aún mas sensibles. El GDPR (“General Data Protection Regulation” o “Regulación UE 679/2016”) de la Unión Europea los referencia expresamente. En dicho reglamento, se define en el art. 4 de la siguiente manera: “*Datos biométricos*” significa datos personales resultantes del procesamiento técnico específico relacionado con las características físicas, fisiológicas o de comportamiento de una persona física, que permiten o confirman la identificación única de esa persona física, como imágenes faciales o datos dactiloscópicos;”. Asimismo, en el Art. 9 del GDPR también se prevé como regla una prohibición que limita el procesamiento y la recolección de esta especial categoría de datos. El art. 9 dice de la siguiente manera: “1. El procesamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, y el

procesamiento de datos genéticos, datos biométricos con el fin de identificar a una persona física, los datos sobre la salud o datos relacionados la vida sexual u orientación sexual de una persona física serán prohibidos.” (el destacado y subrayado es propio)

En el mismo sentido, la Resolución 4 del 2019 de la Agencia de Acceso a la Información Pública aprobó criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley N° 25.326, siendo de observancia obligatoria para todos aquellos sujetos alcanzados por la Ley N° 25.326 -como el demandado-. En dicha resolución se estableció en el criterio interpretativo N° 4 que “[...] *Los datos biométricos que identifican a una persona **se considerarán datos sensibles** (conforme el artículo 2º, 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).*” (el destacado es propio). Esto indica sin lugar a dudas que solamente el titular del dato biométrico puede efectivamente autorizar su uso, y que el Estado tiene que hacer todo lo posible para evitar realizar tratamiento de dichos datos que no sean expresamente autorizados por su titular.

En los regímenes protectores de datos personales de la ciudad y del Estado Nacional, existe el principio mediante el cual el sujeto del cual se extrae el dato personal debe necesariamente proveer su consentimiento expreso. No obstante, existe una excepción que determina que no será necesario ese consentimiento siempre y cuando los datos personales se recaben para el ejercicio de funciones propias de los poderes de la ciudad o del Estado Nacional en su caso. Esta misma excepción es la que utiliza la Resolución 398 en sus considerandos. Dicha resolución establece expresamente “[...] *Que la Ley Nacional N° 25.326 de Protección de los Datos Personales establece que no será necesario el consentimiento del titular de los datos para el tratamiento de los mismos cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; y b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; [...]*”.

Situaciones de similares características y en la cual se han esgrimido los mismos argumentos ya se han planteado en los tribunales. En particular hay un antecedente que se relaciona directamente con el alcance que la excepción esgrimida por el GCBA tiene en lo que respecta a la protección de los datos sensibles de sus ciudadanos. Este antecedente es “INSTITUTO PATRIA PENSAMIENTO ACCION Y TRABAJO PARA LA INCLUSION AMERICANA ASOCIACION CIVIL c/ I.G.J.

1899459/7544628/7734718/921/922 s/RECURSO DIRECTO A CAMARA” (Expte. 8735/2018 CNCIV – Sala L).

La Inspección General de Justicia le exigió al “Instituto PATRIA” la presentación del libro de Registro de Asociados a efectos de poder aprobar el balance del instituto en cuestión. Al realizar esta exigencia, el Instituto Patria manifestó que dicho registro se encontraría amparado por la Ley 25.326 al ser un “dato sensible” que no podía aportar sin el consentimiento de sus titulares. Ante esto, la IGJ argumentó que ese consentimiento no se necesitaba ya que entraría en las excepciones del art. 5 de la Ley 25.326 (datos de acceso público irrestricto y que se recababan para el ejercicio de funciones propias del estado).

Así las cosas, la Sala L de la Cámara Nacional en lo Civil resolvió: “[...] Ello es así, pues si bien es cierto, como puntualiza la I.G.J. al contestar los agravios, que el art. 5 de la ley 25.326 establece excepciones al consentimiento del afectado para el tratamiento de datos; dicha norma legal no resulta de aplicación al caso, pues, como se vio, en la especie se encuentran involucrados datos sensibles de los asociados del Instituto Patria, y los únicos legitimados para develar un dato personalísimo son sus titulares. [...]” “[...] En suma, sin desconocer la función fiscalizadora que la Inspección General de Justicia posee sobre las asociaciones civiles, prevista por los arts. 6 y 10 de la ley 22.315 y por el art. 174 del Código Civil y Comercial de la Nación, respecto de los actos sometidos a su contralor, y aun cuando, como en el caso, sus funciones implicaron poner en juego una actividad jurisdiccional, el cumplimiento de la manda impuesta por la I.G.J. lesiona derechos constitucionales de los asociados del Instituto Patria, como ser el derecho a la intimidad y a la privacidad, a la no discriminación, a la libertad de conciencia y el derecho a asociarse libremente con fines ideológicos amparados por los arts. 14, 16 y 19 de la Constitución Nacional, y en diversos Tratados Internacionales con jerarquía constitucional, arts. 2 y 18 de la Declaración Universal de Derechos Humanos, arts. 2, 5 y 22 de la Declaración Americana de los Derechos y Deberes del Hombre, arts. 11, 12 y 16 de la Convención Americana Sobre los Derechos Humanos y arts. 17, 18, 22 y 26 del Pacto Internacional de Derechos Civiles y Políticos, incorporados por el art. 75 inc. 22 de la Constitución Nacional. Es por ello que la Asociación no puede ser compelida a proporcionar la información requerida, por lo menos con los datos detallados como se exigió, al encontrar su límite en un interés superior de los asociados, que este Tribunal no puede pasar por alto. La restricción contemplada por la

ley 25.326, antes analizada, es el sustento normativo del Instituto Patria para desestimar la solicitud que se le formuló.”¹⁵ (el destacado y subrayado es propio).

En este mismo sentido, los únicos que podrían brindar su consentimiento para que se realice un tratamiento de datos personales de carácter sensible, como es la comparación de datos biométricos con una base de datos previa, son sus propios titulares. Es de destacar que existe la Disposición N° 10/2015 que estableció las “CONDICIONES DE LICITUD PARA LAS ACTIVIDADES DE RECOLECCIÓN Y POSTERIOR TRATAMIENTO DE IMÁGENES DIGITALES DE PERSONAS CON FINES DE SEGURIDAD”. Que si bien, adelantamos que no estamos del todo de acuerdo con varias de sus disposiciones, en dichas condiciones se previó expresamente lo siguiente: “ARTICULO 1°.- (Requisitos de licitud de la recolección).

La recolección de imágenes digitales de las personas a través de cámaras de seguridad será lícita en la medida que cuente con el consentimiento previo e informado del titular del dato en los términos previstos por los artículos 5° y 6° de la Ley N° 25.326.

El cumplimiento del requisito de información previa al titular del dato podrá lograrse a través de carteles que en forma clara indiquen al público la existencia de dichos dispositivos de seguridad (sin que sea necesario precisar su emplazamiento puntual), los fines de la captación de las imágenes y el responsable del tratamiento con su domicilio y datos de contacto para el correcto ejercicio de los derechos por parte del titular del dato.

Siempre y cuando la recolección de las imágenes personales no impliquen una intromisión desproporcionada en su privacidad, no será necesario requerir el consentimiento previo del titular del dato en los siguientes casos:

a) los datos se recolecten con motivo de la realización de un evento privado (se realice o no en espacio público) en el que la recolección de los datos sea efectuada por parte del organizador o responsable del evento; o

b) la recolección de los datos la realice el Estado en el ejercicio de sus funciones, siendo en principio suficiente notificación de los requisitos del artículo 6° de la Ley N° 25.326 su publicación en el Boletín Oficial (conforme artículo 22 de la Ley N° 25.326); sin perjuicio de ello, en las oficinas y/o establecimientos

¹⁵ “INSTITUTO PATRIA PENSAMIENTO ACCIÓN Y TRABAJO PARA LA INCLUSION AMERICANA ASOCIACIÓN CIVIL c/ I.G.J. 1899459/7544628/7734718/921/922 s/RECURSO DIRECTO A CÁMARA” Expte. 8735/2018. CNCIV, Sala L..

públicos deberá hacerse saber dicha recolección conforme lo dispuesto en el segundo párrafo del presente artículo; o

c) los datos se recolecten dentro de un predio de uso propio (por ejemplo: ser propiedad privada, alquilado, concesión pública, etc.) y/o su perímetro sin invadir el espacio de uso público o de terceros, salvo en aquello que resulte una consecuencia inevitable, debiendo restringirlo al mínimo necesario y previendo mecanismos razonables para que el público y/o los terceros se informen de una eventual recolección de su información personal en tales circunstancias.”.

Es decir, ya en una norma que reglamenta precisamente el uso de cámaras de vigilancia se le pone un límite al tratamiento que se pueda realizar de la misma (y todo otro dato que se pueda extraer de ella). Este límite está dado por la “intromisión desproporcionada en su privacidad”. Es claro que pasar de una cámara que solamente toma imágenes a realizar tratamientos complejos con datos obtenidos de esas imágenes implican, casi por definición, una intromisión realmente desproporcionada en la privacidad de mis representados.

Ya lo advertía el Dr. Pettrachi en el fallo “Urteaga, Facundo Raúl c/ Estado Nacional -Estado Mayor Conjunto de las FF.AA.- s/ amparo ley 16.986.” cuando recordando la Sentencia del Tribunal Constitucional Alemán que parió el concepto de “autodeterminación informativa”: *“Este es el proceso que se puede reconocer en la evolución de la jurisprudencia del Tribunal Constitucional alemán, que había sostenido la llamada "teoría de las esferas", según la cual se establecía una protección diferenciada de acuerdo con el mayor o menor grado de afectación de la intimidad, y que fuera elaborada, especialmente, en la sentencia sobre el "Mikrozensus" (BVerfGE 27, 1 y sgtes.; acerca de este concepto, confr. Alexy, R., "Theorie der Grundrechte", 1994, pág. 327). Esta concepción restrictiva, fue abandonada en favor de una tutela considerablemente más amplia, cuyos basamentos quedaron sentados en el fallo conocido como "sentencia del censo" ("Volkszählungsurteil", BVerfGE 65, 1 y sgtes.) [...]”* “[...] El punto fundamental de la argumentación del Bundesverfassungsgericht -el tribunal constitucional alemán- fue la consagración de la ***"autodeterminación informativa"***. Según este concepto es el ciudadano quien debe decidir sobre la cesión y uso de sus datos personales. Este derecho -se dijo- puede ser restringido por medio de una ley por razones de utilidad social, **pero respetando el principio de proporcionalidad y garantizando que no se produzca la vulneración del derecho a la personalidad** (confr. Hassemer, op. cit., págs. 162 y sgtes.). [...]” (el destacado y subrayado es propio).

Como no se le escapará al ilustrado criterio de V.S., la desproporcionalidad que viola el debido proceso sustantivo y que rinde la inconstitucionalidad de la Resolución 398 y la Ley 5688, en los artículos correspondientes, pasa precisamente por el hecho de que el Estado busca proveer de “seguridad” a la población, pero en ese camino, no solamente introduce un elemento riesgoso que en vez de proporcionar seguridad lo que hace es ponernos en una posición mucho más vulnerable, si no que viola los derechos personalísimos más íntimos que puede tener una persona de manera desproporcionada. Tales como el derecho a la privacidad, intimidad y autodeterminación informativa. En el medio, también pasa por arriba casi todo el régimen protectorio de datos personales de forma totalmente ilegítima. Por lo tanto, este es otro argumento que justifica la inconstitucionalidad de la norma objetada en el presente proceso y que V.S. deberá declarar ilegítima e inconstitucional.

En este punto es necesario tener en consideración que lo más importante que se ataca en este apartado es la recolección y tratamiento indiscriminado de rasgos biométricos de mis representados cuando estos transitan por las calles. Sin estar estos registrados en el CONARC y sin tener antecedente criminal alguno. El hecho que el Ministerio tenga o no tenga autorización para realizar el tratamiento de los datos que les remita el RENAPER no implica que estos no necesiten el consentimiento expreso de mis representados para extraer de ellos forzosamente los datos personales sensibles en forma de rasgos biométricos. Por lo tanto, el hecho que el Art. 23 inc. 2 de la Ley 25.326 autorice a las fuerzas de seguridad ha realizar tratamientos sin consentimiento no implica que estos puedan extraer indiscriminadamente datos personales de todas las personas. De lo contrario estaríamos ante una situación completamente desproporcionada que anularía la existencia de cualquier régimen de protección de datos personales.

C. La encriptación/cifrado de la información obtenida y tratada no es la adecuada.

En el pedido de acceso a la información pública que ODIA ha presentado se pudo obtener cierta información acerca de la manera en la cual se guarda la información obtenida y se transmite desde la obtención de la imagen a través de la cámara al Centro de Monitoreo Urbano (de ahora en más “CMU”) donde se realiza el tratamiento de las imágenes y donde *a priori* se utilizaría el Sistema de Reconocimiento Facial de Prófugos.

Así también la asociación logró obtener información acerca de como guardan esa información una vez que la misma llega al CMU para su tratamiento.

De dicha información que ODIA logró obtener surge con claridad que los sistemas de cifrado utilizados por el GCBA para transmitir las imágenes y guardar dichas imágenes es un protocolo de encriptación sumamente vulnerable que pone en riesgo los datos ilegítimamente obtenidos.

Le advierto a V.S. que este apartado puede parecer algo técnico, no obstante, es necesario adentrarnos ligeramente en las tecnologías usadas para proteger la información obtenida de manera de poder determinar si dicha información está siendo protegida correctamente y si permanecerá confidencial. Recordemos que estamos hablando de datos biométricos relativos a personas físicas. Es decir, datos que merecen la mayor de las protecciones, tanto técnicas como jurídicas. En este sentido, piense V.S. que una contraseña puede cambiarse en el caso de verse la misma vulnerada, sin embargo, los datos biométricos de una cara no.

La etimología del verbo cifrar deriva de la del verbo “encriptar”. Dicha palabra es un neologismo derivado de la palabra en inglés “to encrypt” que a su vez tiene como fuente el verbo griego ἐγκρύπτω ("enkρύpto") que significa esconder una cosa dentro de otra. Este verbo griego está a su vez compuesto del prefijo ἐν que significa “en” y el verbo κρύπτω que significa “ocultar”.

En este sentido, cuando hablamos del cifrado de la información obtenida por las cámaras que después va a ser tratada en el CMU y de donde surgirán (o no) las correspondientes alertas que motivaran el accionar del poder de policía del estado, **hablamos sobre la manera en la cual esa información utilizada es guardada de manera “confidencial” u “oculta” a cualquier otra persona que no se encuentre autorizada para acceder a esa información.**

Asimismo, en asuntos de seguridad informática hay dos momentos en los cuales se debe tener especial cuidado con la información que se obtenga. Estos dos momentos son 1) en el tránsito que tiene la información desde su captura hasta su lugar de tratamiento; y 2) una vez haya arribado a su lugar de tratamiento, de que manera se guarda en los servidores (computadoras) que realizan ese tratamiento.

En ese orden de ideas, una de las preguntas que hizo la asociación “ODIA” (y que fuera contestada a través de la NO-2019-37063734-GCABA-DGEYTI del Jueves 28 de noviembre de 2019.) fue la siguiente: “10) *¿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?” a esto el GCBA contestó “La información desde que es capturadas hasta que llega al CMU, viaja encriptado mediante aplicabilidad del protocolo 3DES.”(el destacado es propio).

De la misma manera, por medio de la nota NO-2019-33745359-GCABA-DGEYTI de fecha miércoles 30 de octubre 2019 se preguntó: “15) 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?” sencillamente se el GCBA contestó “Se utiliza un cifrado 3 DES”.

Por lo tanto V.S. parecería quedar claro que el protocolo de encriptación elegido para tanto la transmisión de los datos obtenidos por las cámaras como para el almacenamiento de las mismas en el CMU es el protocolo 3DES. No obstante, es necesario destacar el que el protocolo de encriptación elegido para realizar el cifrado de la información obtenida es sumamente inseguro y así ha sido destacado por organismos especializados.

Para empezar, este tipo de cifrado es del tipo “simétrico”. El cifrado simétrico es aquel mediante el cual se utiliza solamente una clave para cifrar y descifrar la información encriptada. En este sentido, se entiende de estas respuestas que las imágenes obtenidas por las cámaras son cifradas con un clave y al momento de llegar al CMU son descifradas con la misma clave. En este sentido, cualquier persona que tenga al alcance dicha clave podrá capturar esa información en cualquier lugar desde la transmisión hasta el almacenamiento de esos datos y descifrarlos. Esto, en contraposición al uso de tecnologías de cifrado “asimétrico” donde existe una clave con la que se encripta cuya reserva o seguridad no es necesaria (se la conoce como clave pública) y por el contrario, puede ser descryptada solamente con lo que se llama la “clave privada” que solamente aquel que recibe la información debe conocer.

En este sentido, un sistema de encriptación de clave pública-privada debería ser el adecuado para asegurar una mejor protección y confidencialidad ya que las cámaras, al ser tantas y encontrándose libres alrededor de la Ciudad de Buenos Aires, se exponen a ataques de seguridad en el cual se intenten obtener las claves de esas cámaras y de esa manera poder obtener acceso remoto a las mismas. Por lo tanto, si se utiliza un sistema de encriptación simétrico, con el mero conocimiento de la clave en alguna de las cámaras se podrá acceder a la información recopilada por ella. Por el contrario, si se utiliza un sistema de encriptación asimétrico, el único que estaría posibilitado de acceder a la

información provista por estas cámaras, sería el destinatario de las imágenes (en nuestro caso el CMU). Sin ir más lejos, existen páginas web como <http://insecam.org/en/bycountry/AR/?page=1> en donde se puede tener acceso a muchas cámaras que apuntan hacia las calles de la ciudad de buenos aires de manera remota, lo cual demuestra lo altamente vulnerable que son las mismas.

Por el otro lado, el protocolo 3DES de encriptación es sumamente susceptible de ser atacado por “fuerza bruta”. Esto quiere decir, básicamente, que un atacante podría acceder a la información encriptada probando aleatoriamente claves hasta que logre obtener aquella que le permita acceder a la información. En este sentido el NIST o “National Institute of Standards and Technology” del Departamento de Comercio de los Estados Unidos ya ha realizado determinadas advertencias en la línea de que no se debe usar este protocolo de encriptación¹⁶.

Asimismo, Apple Inc. ha dejado de utilizar 3DES como sistema de encriptación seguro.¹⁷ Microsoft ha retirado 3DES como algoritmo de encriptación seguro¹⁸. Lo mismo ha hecho Mozilla (la empresa detrás del navegador “Firefox”)¹⁹ y muchas otras empresas han seguido este camino.

Así también los investigadores y científicos Karthikeyan Bhargavan y Gaëtan Leurent han demostrado empíricamente la debilidad de este sistema de encriptación de la información con su ataque de “los dulces 32”²⁰.

Si bien no existe normativa a nivel de la Ciudad de Buenos Aires que establezca cuales son las medidas de seguridad adecuadas para el almacenamiento de este tipo de datos personales, a nivel federal existe la Resolución 47/2018 de la Agencia de Acceso a la Información Pública. Por medio de esa resolución se aprobaron las “Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios informatizado”.

En dicha resolución se “recomienda” que todos aquellos que manejen bases de datos deben **Asegurar la confidencialidad** durante todo el proceso de recolección. Esto, con el protocolo 3DES de encriptación NO sucede. Este es un argumento que se suma a

¹⁶ Ver <https://csrc.nist.gov/news/2017/update-to-current-use-and-deprecation-of-tdea> donde se advierte “NIST insta a todos los usuarios de TDEA a migrar a AES lo antes posible.”

¹⁷ <https://developer.apple.com/forums/thread/89272> “El problema más inmediato es que estás utilizando 3DES el cual ya no es considerado seguro”

¹⁸ Ver <https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/3155527?redirectedfrom=MSDN>

¹⁹ Ver “Triple DES is weak” https://bugzilla.mozilla.org/show_bug.cgi?id=1267899

²⁰ Ver más <https://sweet32.info/>

los fundamentos por los cuales este SRFP debería ser declarado inconstitucional y contrario a las normas de protección de los datos personales de mis representados.

D. Discriminación

Como V.S. sabe, existen en nuestro país normas y doctrinas que luchan contra la discriminación. Para empezar nuestra propia Constitución Nacional establece en diversos apartados el derecho a la igualdad (igualdad de oportunidades, la inexistencia de fueros personales, etc.). Además de ello, en el art. 75 inc. 22 de nuestra CN, se extendió nuestra estructura constitucional a los distintos tratados internacionales de derechos humanos que expresamente establecen disposiciones antidiscriminatorias. Así, por ejemplo, la Declaración Universal de los Derechos Humanos de 1948 establece expresamente “[...] *Artículo 7. Todos son iguales ante la ley y tienen, sin distinción, derecho a igual protección de la ley. Todos tienen derecho a igual protección contra toda discriminación que infrinja esta Declaración y contra toda provocación a tal discriminación. [...]*”. El Pacto Internacional de Derechos Civiles y Políticos de 1966 establece “[...] *Artículo 26 Todas las personas son iguales ante la ley y tienen derecho sin discriminación a igual protección de la ley. A este respecto, la ley prohibirá toda discriminación y garantizará a todas las personas protección igual y efectiva contra cualquier discriminación por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social. [...]*”. Asimismo, el Pacto Internacional de Derechos Económicos Sociales y Culturales de 1966 dispone “[...] *2. Los Estados Partes en el presente Pacto se comprometen a garantizar el ejercicio de los derechos que en él se enuncian, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social. [...]*”. Así también la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial de 1965 determina “[...] *Artículo 1 1. En la presente Convención la expresión “discriminación racial” denotará toda distinción, exclusión, restricción o preferencia basada en motivos de raza, color, linaje u origen nacional o étnico que tenga por objeto o por resultado anular o menoscabar el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos humanos y libertades fundamentales en las esferas política, económica, social, cultural o en cualquier otra esfera de la vida pública. [...]*”. En adición la Convención

Americana sobre Derechos Humanos de 1969 establece “[...]Artículo 1. Obligación de Respetar los Derechos 1. Los Estados Partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social. [...]” “[...] Artículo 24. Igualdad ante la Ley. Todas las personas son iguales ante la ley. En consecuencia, tienen derecho, sin discriminación, a igual protección de la ley [...]”. Si bien existen otros tratados, artículos y convenciones que podría citar, me parece que queda claro que la lucha en contra de la discriminación es algo que nuestro plexo constitucional no solo busca si no que ordena e instruye. En este sentido, incorporar una tecnología que es discriminatoria y que tiene consecuencias gravísimas como la vulneración de la libertad ambulatoria de las personas, es profundamente inconstitucional y viola aquellos derechos personalísimos de los ciudadanos que más protección merecen. Sin ir más lejos, nuestra propia Corte Suprema de Justicia de la Nación ha establecido que las normas antidiscriminatorias son de carácter *ius cogens* y su violación hace nulo el acto atacado: “A ello se suma, por cierto, que la necesaria adecuación de los remedios en los términos ya indicados, prenda de su imprescindible efectividad, adquiere todavía más entidad en casos como el presente, esto es, cuando el agravio puesto en la liza judicial involucra a los principios de igualdad y de prohibición de toda discriminación, por cuanto estos resultan elementos arquitectónicos del orden jurídico constitucional argentino e internacional (Constitución Nacional, art. 16; Declaración Americana de los Derechos y Deberes del Hombre, art. 2; Declaración Universal de Derechos Humanos, arts. 2 y 7; Pacto Internacional de Derechos Civiles y Políticos, arts. 2.1 y 26; PIDESC, arts. 2º y 3º, y Convención Americana sobre Derechos Humanos, arts. 1.1 y 24, además de los tratados destinados a la materia en campos específicos: Convención sobre la Eliminación de todas las Formas de Discriminación Racial; Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer, esp. arts. 2, 3 y 5 a 16, y Convención sobre los Derechos del Niño, art. 2º). Tanto es así que, de acuerdo con lo sostenido por el Tribunal en *Álvarez, Maximiliano c/ Cencosud SA* (Fallos: 333:2306, 2313/2315, 2320, 2323 - 2010), los mentados principios han alcanzado la preeminente categoría de *ius cogens*, según lo ha esclarecido la Corte Interamericana de Derechos Humanos (Condición Jurídica y Derechos de los Migrantes Indocumentados, Opinión Consultiva

OC-18/03 del 17 de septiembre de 2003, Serie A N° 18, párrs. 97/101 y 110), lo cual acentúa, para el Estado, la **“obligación fundamental mínima” y de cumplimiento “inmediato” de garantizar la no discriminación**, cuya inobservancia, por acción u omisión, lo haría incurrir en un acto ilícito internacional (Comité de Derechos Económicos, Sociales y Culturales, Observación general N° 18. El Derecho al Trabajo, 2005, párrs. 31 y 18), cuanto más que aquél ha asumido la obligación de “proteger” los derechos humanos, esto es, el deber de adoptar las “medidas que impidan a terceros interferir en el disfrute del derecho al trabajo” (idem, párr. 22).”²¹

No obstante, para poder empezar a profundizar en esta materia lo suficiente es necesario que V.S. entienda como funciona este sistema. En este sentido, la Resolución 398, que luego inspiró la Ley 5688 en sus artículos pertinentes, dispone y explica: “[...] Que en tal sentido, se ha desarrollado el Sistema de Reconocimiento Facial de Prófugos, como un instrumento comprendido dentro del Sistema Público de Video Vigilancia de la Ciudad Autónoma de Buenos Aires, el cual mediante una cámara de video vigilancia reconoce los rostros de las personas requeridas por orden judicial, registradas en las Bases de Datos del Sistema de Consulta Nacional de Rebeldías y Capturas (CONARC) del Registro de Reincidencia del Ministerio de Justicia y Derechos Humanos de la Nación; [...]”. Esto quiere decir, V.S. que el MJYSGC toma imágenes del “Sistema Público de Video Vigilancia” de la C.A.B.A. y los procesa a través de este SRFP. ¿Y de que manera los procesa? Básicamente el sistema toma los datos de las personas que se encuentran en el CONARC (y otras aquellas personas que el Ministerio solicite) y el MJYSGC solicita al Registro Nacional de las Personas que les mande las imágenes de aquellas personas que se encuentra en ese listado. Este procedimiento surge con claridad en el Convenio firmado entre el Ministerio y el RENAPER que adjunto al presente como **Anexo III**. En dicho convenio se establece en su cláusula segunda “[...] SEGUNDA: El RENAPER facilitará, por la vía de excepción prevista en el artículo 23, inciso 2) de la Ley N° 25.326, el acceso a la información disponible en sus sistemas informáticos tendiente a identificar y/o verificar la identidad de las personas humanas sobre las cuales el MINISTERIO desarrolle las tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial nacional, provincial y de la Ciudad Autónoma de Buenos Aires, y durante la etapa de prevención e investigación de delitos de acción pública con arreglo a lo dispuesto en los artículos 184 del Código Procesal Penal de la Nación y 84 del Código

²¹ P. 489. XLIV. Pellicori, Liliana Silvia c/ Colegio Público de Abogados de la Capital Federal s/ amparo. Fallos: 334:1387. C.S.J.N.

Procesal Penal Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires. Para dicha tarea, el RENAPER facilitará las fotografías del listado de personas que el MINISTERIO le requiera, indicando este último el nombre y Documento Nacional de Identidad que corresponda a cada una de ellas. [...]” (el destacado es propio). Una vez obtenidas dichas imágenes, el SRFP buscará entre todas las caras que se obtengan de las imágenes del Sistema Público de Video Vigilancia las caras de aquellas fotos que el RENAPER haya mandado. Sin embargo, ¿Cómo sabe el sistema que es una cara? O más aún, ¿Qué buscar en una cara para asegurarse de estar identificando a alguien correctamente? El Pliego de Especificaciones Técnicas mediante el cual se realizó la Contratación Directa de este SRFP lo establece no con demasiada claridad: *“Dicho servicio tendrá como objetivo el análisis inteligente en tiempo real sobre imágenes de video en vivo para la detección facial de personas buscadas basada en bases de datos de imágenes de rostros y de análisis inteligente de video para la detección de diferentes patrones de comportamiento y cambios de condiciones ambientales, más adelante descriptos en el presente documento. Dicho servicio será prestado sobre todas las cámaras de video vigilancia que técnicamente lo permitan, como así también a las imágenes almacenadas en los sistemas de resguardo de imágenes.”* (el destacado y subrayado es propio).

¿Qué quiere decir este “análisis inteligente”? Como no se le escapará al ilustrado criterio de V.S. este concepto es absolutamente esencial para determinar como funciona este sistema. Ya que, si no entendemos de que manera funciona este “análisis inteligente” no podremos entender cual es el racional detrás del funcionamiento de este sistema y de que manera toma la decisión de levantar una alerta cuando “percibe” que ha encontrado una cara. No obstante, en ninguna parte del pliego de contratación ni en ninguna parte de las especificaciones técnicas se explica en que consiste este análisis “inteligente”. Por esta razón, ODIA habría realizado, en su solicitud de Acceso a la Información Pública las siguientes preguntas: “[...] 61) ¿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? [...]” A esta pregunto el GCBA contestó en instancia administrativa (NO-2019-25581723-GCABA-DGEYTI) lo siguiente: *“Esta información corresponde al desarrollo del producto y es un detalle que posee el copyright de la licencia del mismo, por lo cual no se posee acceso a esta información.”*. Así también ODIA habría consultado: “[...] 62) ¿Qué datasets fueron utilizados para ese

entrenamiento y que organismo fue responsable? [...]” la escueta respuesta fue la siguiente “Ver respuesta 61.”.

En instancia judicial, la respuesta del GCBA, a la pregunta 61 de ODIA, se respondió (NO-2019-33745359-GCABA-DGEYTI) lo siguiente: “[...] *Se realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los caso los porcentajes de error exigidos [...]*”. Asimismo, surge del expediente en cuestión que en un traslado posterior del GCBA (NO-2019-37063734-GCABA-DGEYTI, **Anexo IV**) se habría hecho saber lo siguiente “*Dependiendo de la calidad de las imágenes obtenidas del cruzamiento de la base de datos del CONARC con el RENAPER, se utiliza alguno de los métodos siguientes: holístico, locales o Geométricos.*”

Como set de datos para calibrar y verificar el funcionamiento del sistema, se realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los casos los porcentajes de error exigidos.” (el destacado es propio) Asimismo, a la pregunta N° 62 se nos contestó nuevamente con una copia de la segunda parte de la respuesta de la pregunta 61.

No obstante, el hecho que se utilicen esos tres métodos para realizar el reconocimiento facial, son una fuente de información de una importancia inconmesurable. Esto así por que prueba, sin lugar a dudas, la inconstitucionalidad por discriminación que realiza este SRFP. Un método holístico²², local geométrico²³ de reconocimiento facial funciona utilizando información previamente obtenida de una gran cantidad de imágenes. Es decir, que las fotos obtenidas del RENAPER no se contrastan solamente con las imágenes obtenidas de las cámaras, si no que para que el sistema “entienda” que es lo que está buscando, debe necesariamente haber aprendido, mediante el uso de una cantidad de imágenes de terceros, que es lo que debe buscar en una cara. Para ello, se utilizan millones de imágenes que pasan por este sistema, de manera que el mismo aprenda por si solo que es lo que debe buscar en una cara. Sin embargo, lo cierto es que, si el sistema fue entrenado para ser utilizado en una población con demografías distintas, entonces es muy probable que ese sistema sea menos eficaz.

²² Sasan Karamizadeh, Shahidan M. Abdullah y Mazdak Zamani “*An Overview of Holistic Face Recognition*” IJRCCT. International Journal of Research in Computer & Communication Technology. ISSN 2278-5841

²³ Vikas Maheshkara, Suneeta Agarwalb, Vinay Kr. Srivastavac Sushila Maheshkard “*Face Recognition using Geometric Measurements, Directional Edges and Directional Multiresolution Information*”. Publicado por Elsevier Ltd.

En este sentido, se han hecho una gran cantidad de estudios sobre este tipo de tecnologías que han demostrado con certeza científica que el uso de este tipo de tecnologías es discriminatorio. Por ejemplo, en un estudio del año 2012, el cual tuvo como co-autor al FBI²⁴ estadounidense y se estudió a los tres algoritmos de Reconocimiento Facial comerciales más estudiados se concluyó “[...] *Las actuaciones de los tres algoritmos comerciales estudiados fueron consistentes en que todos ellos exhibieron menores precisiones de reconocimiento en las siguientes cohortes: mujeres, negros y sujetos más jóvenes (18 a 30 años).* [...]” (el destacado es propio).

En otro estudio del Massachusetts Institute of Technology del año 2018²⁵ se descubrió con datos duros, en otros tres sistemas de reconocimiento facial lo siguiente:

“[...] • *Todos los clasificadores funcionan mejor en rostros masculinos que las caras femeninas (8.1% - 20.6% de diferencia en tasa de error)*

• *Todos los clasificadores funcionan mejor en caras más claras que las caras más oscuras (11.8% - 19.2% de diferencia en tasa de error)*

• *Todos los clasificadores tienen su peor desempeño con las caras de las mujeres más oscuras (tasa de error del 20.8% - 34.7%) [...]*”

Es decir V.S., de tres de los MEJORES algoritmos de reconocimiento facial a los cuales se pueden acceder en el mercado, los TRES demostraron serias dificultades para reconocer correctamente a personas de minorías raciales. Esto quiere decir V.S. que el SRFP no solo pone en riesgo a mis representados que circulan por nuestra Ciudad si no que pone en una vulnerabilidad mucho más profunda a la que ya está en una situación vulnerable. En este caso, con las mujeres de color.

Pero esto no es todo V.S., el NIST de los Estados Unidos, en diciembre del año 2019²⁶ hizo su propio estudio sobre como afecta la demografía a los distintos proveedores de algoritmos de reconocimiento facial. En dicho estudio se concluyó que las personas asiáticas, afroamericanas y nativo-americanas tenían hasta 100 veces más probabilidades de ser identificadas erróneamente por reconocimiento facial que los hombres blancos. Las mujeres tenían más probabilidades de ser identificadas falsamente que los hombres, y los

²⁴ Brendan F. Klare, Member, IEEE, Mark J. Burge, Senior Member, IEEE, Joshua C. Klontz, Richard W. Vorder Bruegge, Member, IEEE, and Anil K. Jain, Fellow, IEEE “Face Recognition Performance: Role of Demographic Information” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 6, DECEMBER 2012.

²⁵ Joy Buolamwini y Timnit Gebru “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification”. <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

²⁶ Se puede acceder al estudio completo en el siguiente link <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

ancianos y los niños tenían más probabilidades de ser identificados erróneamente que los de otros grupos de edad. Los hombres blancos de mediana edad generalmente se beneficiaron de las tasas de precisión más altas.

Lo cierto es V.S. que es difícil encontrar más ejemplos que demuestren lo increíblemente injusto que significa implementar un SRFP que no solo funciona mal si no que es discriminatorio con las personas que nunca deberían serlo. Es decir, a las mujeres - como una de mis representadas-, a las personas de distintas etnias y a los niños y ancianos. A las personas que con más ímpetu el estado debería proteger.

Así, en la doctrina nacional no se le ha escapado dicha situación. De esa manera se ha dicho que “[...] *También en los sistemas de reconocimiento facial existen riesgos o peligros, cuando por ejemplo presentan problemas para reconocer caras de personas de determinado color de piel, y esto tiene que ver con la incorporación previa de datos con los que se dotó al sistema*. Cuando se habla de lo exitosos que son estos sistemas porque poseen un 70% de efectividad, nadie piensa que de manera absolutamente ilegal se ha procedido injustamente afectando la libertad de ese 30% de personas respecto de las cuales el reconocimiento falló. [...]”²⁷. (el destacado y subrayado es propio)

La inconstitucionalidad por discriminación en violación a la garantía de igualdad de nuestro plexo constitucional viene de la mano del hecho de implementar un Sistema de Reconocimiento Facial de Prófugos que levanta alertas y reconoce como “prófugos” a personas con rasgos demográficos minoritarios. Esto ha sido extensamente probado en publicaciones científicas especializadas como lo hemos visto hasta el momento y sugiere que la cantidad de casos de falsos positivos que han surgido por el uso de este sistema en las calles de la Ciudad se deben precisamente a esta situación. **V.S., no podemos permitir en un Estado de Derecho que este tipo de tecnologías se utilicen.**

Sin ir más lejos, no solamente nuestro plexo constitucional prohíbe este tipo de discriminaciones, si no que también tenemos una ley federal que expresamente prohíbe este tipo de actos. El art. 1 de la Ley 23592 determina que “**ARTICULO 1º.- Quien arbitrariamente impida, obstruya, restrinja o de algún modo menoscabe el pleno ejercicio sobre bases igualitarias de los derechos y garantías fundamentales reconocidos en la Constitución Nacional, será obligado, a pedido del damnificado, a**

²⁷ LOPEZ, Maria Elena “INTELIGENCIA ARTIFICIAL: UNA IMPORTANTE HERRAMIENTA DE GESTIÓN SI SE REGULA DESDE LA ÉTICA” Publicado en: RDLSS 2019-24 , 2491 Cita Online: AR/DOC/3819/2019. La Ley.

dejar sin efecto el acto discriminatorio o cesar en su realización y a reparar el daño moral y material ocasionados.

A los efectos del presente artículo se considerarán particularmente los actos u omisiones discriminatorios determinados por motivos tales como raza, religión, nacionalidad, ideología, opinión política o gremial, sexo, posición económica, condición social o caracteres físicos. [...]”

La situación explicada hasta el momento entra en contradicción perfecta contra la Ley 23592. Esto así por que se constituye en una situación discriminación indirecta. Las Observaciones Generales Aprobadas Por el Comité de Derechos Económicos, Sociales y Culturales explican detalladamente que puede constituir una “Discriminación Indirecta”. Así, se dijo que “[...] 13. *Se produce discriminación indirecta cuando la ley, el principio o el programa no tienen apariencia discriminatoria, pero producen discriminación en su aplicación. Ello puede suceder, por ejemplo, cuando las mujeres están en situación desfavorable frente a los hombres en lo que concierne al disfrute de una oportunidad o beneficio particulares a causa de desigualdades preexistentes. La aplicación de una ley neutra en cuanto al genero puede perpetuar la desigualdad existente o agravarla. [...]*”.²⁸

Así también, estas observaciones han establecido “10. [...] b) *La discriminación indirecta hace referencia a leyes, políticas o prácticas en apariencia neutras pero que influyen de manera desproporcionada en los derechos del Pacto afectados por los motivos prohibidos de discriminación. Por ejemplo, exigir una partida de nacimiento para poder matricularse en una escuela puede ser una forma de discriminar a las minorías étnicas o a los no nacionales que no posean, o a quienes se hayan denegado, esas partidas. [...]*”²⁹

“[...] 12. *El Comité ha constatado periódicamente que la discriminación contra algunos grupos subsiste, es omnipresente, está fuertemente arraigada en el comportamiento y la organización de la sociedad y a menudo implica actos de discriminación indirecta o no cuestionada. Esta discriminación sistémica puede consistir en normas legales, políticas, prácticas o actitudes culturales predominantes en el sector público o privado que generan desventajas comparativas para algunos grupos y privilegios para otros. [...]*”.³⁰

²⁸ Observación general N° 16. “La igualdad de derechos del hombre y la mujer al disfrute de los derechos económicos, sociales y culturales”.

²⁹ Observación general N° 20 “La no discriminación y los derechos económicos, sociales y culturales (artículo 2, párrafo 2 del Pacto Internacional de Derechos Económicos, Sociales y Culturales)”

³⁰ Idem.

En este mismo sentido, la discriminación indirecta que proviene de este SRFP pasa por el hecho de que los efectos que tiene este sistema son particularmente lesivos para la población más vulnerable. Además de ello, también es necesario destacar que este SRFP en nada ayuda a transformar la discriminación estructural que usualmente sufren aquellas personas que cometen delitos. Es decir, aún asumiendo que este sistema funcione perfectamente y que los datos obtenidos por el sean guardados con la suficiente seguridad, lo cierto es que el sistema no ayuda a resolver el verdadero problema. Es decir, la desigualdad de oportunidades, las crisis económicas y el resto de los factores que ponen en situaciones aún más vulnerables a la población.

No obstante, lo cierto es que a lo largo de esta presentación se ha superado el estándar probatorio requerido para acreditar prima facie que la implementación de este Sistema de Reconocimiento Facial de Prófugos es discriminatoria. No obstante, es nuestro deber destacar que nuestra C.S.J.N. ha advertido que la prueba del acto discriminatorio, si bien recae sobre quien lo alega, es sumamente difícil. En ese sentido, nuestra Corte ha señalado que esta dificultad radica en el hecho que usualmente los archivos y la información que serían necesarios para acreditar dicho acto discriminatorio suelen estar en manos de quien realiza, precisamente, el acto discriminatorio.³¹ Sin embargo, nuestra CSJN ha resuelto que **“[...] Así, a modo de conclusión, resultará suficiente, para la parte que afirma dicho motivo, con la acreditación de hechos que, prima facie evaluados, resulten idóneos para inducir su existencia, caso en el cual corresponderá al demandado a quien se reprocha la comisión del trato impugnado, la prueba de que éste - el acto discriminatorio- tuvo como causa un motivo objetivo y razonable ajeno a toda discriminación. La evaluación de uno y otro extremo, naturalmente, es cometido propio de los jueces de la causa, a ser cumplido de conformidad con las reglas de la sana crítica. [...]”**³².

Todo esto sucede en un contexto donde se sabe que las fuerzas policiales utilizan perfiles raciales y étnicos para realizar detenciones arbitrarias. Esto ha sido constatado por el *Special Rapporteur* de las Naciones Unidas Mutuma Ruteere: “16. Los agentes de policía y de inmigración y los funcionarios de prisiones a menudo actúan basándose en perfiles raciales y étnicos, en muchas formas distintas y perniciosas. También puede suceder que las políticas oficiales faciliten prácticas discrecionales que permiten que las

³¹ ³¹ P. 489. XLIV. Pellicori, Liliana Silvia c/ Colegio Público de Abogados de la Capital Federal s/ amparo. Fallos: 334:1387. C.S.J.N.

³² Idem.

*autoridades encargadas de hacer cumplir la ley dirijan selectivamente sus actuaciones hacia grupos o personas basándose en el color de su piel, en su vestimenta, en su vello facial o en el idioma que hablan. A veces también existe un sesgo implícito que motiva la utilización de criterios raciales y étnicos en la actuación de las fuerzas del orden. Aunque algunos estudios han demostrado la ineficacia de la utilización de perfiles raciales y étnica, los funcionarios siguen recurriendo a esa práctica. Una de sus manifestaciones es la práctica de la interceptación y cacheo o la interceptación e identificación especialmente dirigidas contra minorías. Esta práctica tiene como resultado un número desproporcionadamente alto de actuaciones contra esas poblaciones a menudo vulnerables.”*³³

En este sentido V.S., en virtud de lo expuesto en los apartados anteriores, la Resolución 398 y la Ley 5688 modificada por la ley 6339 que ha implementado este sistema discriminatorio es completamente nula e inconstitucional. Es por ello que le solicitamos a V.S. que así lo disponga y utilice estos argumentos cuando resuelva el fondo del asunto y cuando le toque expedirse sobre la medida cautelar solicitada por la Asociación Civil ODIA.

E. Sobre el caso *R (on the application of Bridges) v. Chief Constable of South Wales Police*.

El caso referenciado en este subtítulo es uno de los primeros casos en el mundo donde se ha evaluado la legalidad de un Sistema de Reconocimiento Facial y es sumamente importante a efectos de hacer el posible control de convencionalidad entre las leyes atacadas en el presente y nuestro Sistema Interamericano de Derechos Humanos que nuestro país se ha comprometido a proteger. En resumen, en dicho fallo la Cámara de Apelaciones decidió que el SRF era violatorio del art. 8 de la Convención Europea de Derechos Humanos (CEDH) que se lee de la siguiente manera:

“ARTÍCULO 8

Derecho al respeto a la vida privada y familiar

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto y en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el

³³ Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Mutuma Ruteere A/HRC/29/46

bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.”

Los argumentos para considerar que este SRF era violatorio al artículo de esta convención fueron básicamente tres: (1) No tenía una base legal (violatorio al principio de legalidad); (2) La Evaluación de Impacto a la Privacidad realizada fue deficiente al evaluar los derechos y libertades de aquellas personas que son procesadas por el SRF; y (3) El SRF no cumplió con el deber de no discriminación que impone la Legislación local del Reino Unido. A continuación procederemos a explicar y desempacar cada uno de esos elementos y haremos una comparación con lo que dispone nuestra Convención Americana de Derechos Humanos (CADH) para que V.S. entienda las razones por las cuales el SRFP de la CABA es inconstitucional y contrario a la CADH.

Sin ir más lejos, nuestra CADH establece en su Artículo 11 lo siguiente:

“Artículo 11. Protección de la honra y de la dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.”

En este sentido, note V.S. que nuestra CADH, así como lo reconoce la CEDH, reconoce el derecho a la vida privada de las personas y protege este derecho contra cualquier injerencia arbitraria o abusiva contra esa injerencia. La Corte Interamericana de Derechos Humanos (CtIDH) lo ha dicho claramente:

“[...]194. La Corte considera que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. [...]”³⁴

*“[...] 48. Por su parte, el artículo 11 de la Convención Americana reconoce que toda persona tiene, entre otros, derecho a la vida privada **y prohíbe toda injerencia arbitraria o abusiva en ella**, enunciando diversos ámbitos de la misma como la vida privada de sus familias, sus domicilios o sus correspondencias. El ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública y comprende, entre otras dimensiones, tomar decisiones relacionadas con diversas áreas de la propia vida*

³⁴ CORTE INTERAMERICANA DE DERECHOS HUMANOS “CASO DE LAS MASACRES DE ITUANGO VS. COLOMBIA” SENTENCIA DE 1 DE JULIO DE 2006

libremente, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público. [...]”³⁵ (el destacado y subrayado es propio)

Visto que tanto nuestra CADH como la CEDH buscan proteger el ámbito de la vida privada de las personas de manera similar, ahora nos adentraremos en los hechos del caso para que V.S. pueda encontrar paralelismos que le permitan entender por que el SRFP de la CABA es inconstitucional por ser contrario a la CADH.

El Sr. Bridges es un individuo del sur de Gales (parte del Reino Unido) así como mis representados son ciudadanos de esta Ciudad Autónoma de Buenos Aires. El demandado, la Policía del Sur de Gales (“PSG”), es una policía que fue líder en el uso del SRF en cuestión (llamado AFR Locate) que habría sido provisto por la empresa “North Gate Public Services (UK) Ltd” más conocida como NEC. La manera en la cual funcionaría este sistema se encuentra en la sentencia pero básicamente, habría una lista de personas con sus correspondientes imágenes que sería mantenido por la PSG (de manera muy similar a la lista realizada por el CONARC). En dicha lista se incluirían a las siguientes categorías de personas: 1) Personas con pedidos de capturas (warrants); 2) Individuos que se encuentren prófugos de la justicia; 3) Personas sospechadas de haber cometido crímenes; 4) Personas que haya que “cuidar” (missing persons o “desaparecidos”); 5) Individuos cuya presencia en un evento particular sea una fuente de preocupación; 6) personas de interés para la policía y 7) Personas vulnerables.

Las imágenes de cada una de estas personas que forman parte de la lista son procesadas a los efectos de extraer las diferencias biométricas de sus rostros. Una vez hecho esto, el SRF las cámaras utilizadas obtienen las imágenes de todas aquellas personas que circulan por el lugar donde se encuentren y aíslan en tiempo real las imágenes de sus caras obteniendo también distintos rasgos biométricos de todas las personas que son capturadas con las cámaras. Posteriormente, estos rasgos biométricos realizados en tiempo real se comparan con los rasgos biométricos de las caras que forman parte de la lista realizada por la Policía y se obtiene una especie de “puntaje de similitud”. Mientras más alto sea este puntaje más probable es que la persona capturada por la imagen sea alguien que efectivamente se encuentra en esta lista. Note V.S. que esta manera en la cual funciona el SRF Galés es idéntico a como estaría diseñado el SRFP de esta CABA.

³⁵ CORTE INTERAMERICANA DE DERECHOS HUMANOS “CASO FONTEVECCHIA Y D’AMICO VS. ARGENTINA” SENTENCIA DE 29 DE NOVIEMBRE DE 2011

El Sr. Bridges alegó que su cara habría sido identificada por el AFR Locate en diciembre de 2017 en la ciudad de Cardiff y en marzo de 2018 en una protesta. El buscaba que se declarara la no compatibilidad de esta tecnología con el Art. 8 de la CEDH que ya he citado y que el sistema era violatorio del marco protectorio de Datos Personales Inglés. Después de la sentencia de primera instancia, el fallo fue apelado y llegó a las manos de la Cámara de Apelaciones. Que consideró que el SRF en cuestión violaba el Art. 8 de la CEDH conforme los argumentos que hemos descripto anteriormente.

E.1. La Falta de Base Legal suficiente

En lo que hace a este argumento en particular, la Cámara de Apelaciones apoyándose en el antecedente británico *R (Wood) v Metropolitan Police Commissioner* que estableció que para que la injerencia en la vida privada sea legítima la “previsión de la ley” que requiere el Art. 8 de la CEDH debería cumplir con cierto requisito de calidad. Es decir, para que la ley no sea violatoria de dicho artículo de la CEDH, la ley tiene que ser de calidad. En otras palabras, mientras más intrusiva sea la injerencia en la vida privada del individuo, la ley tiene que ser más específica y precisa para justificar dicha injerencia. En este orden de cosas la Cámara de Apelaciones encontró dos deficiencias fundamentales en el armado normativo que justificaba el SRF Galés. En primer lugar no se determinó con suficiente especificidad quien puede ser puesto en esa lista de la PSG y tampoco se dispuso específicamente donde podía emplearse este SRF. Para ello, la Cámara tuvo como especialmente relevante el hecho que la lista podía ser formada por toda aquella persona que sea “de interés” para la PSG lo que le da un ámbito de discreción completamente intolerable. En este mismo sentido, note V.S. que el SRFP de la CABA también adolece de este mismo problema. Si bien el mismo parecería buscar solamente a aquellas personas que se encuentren “prófugas de la justicia”, lo cierto es que también permite buscar personas requeridas por el “Poder Judicial de la Nación, Provincial, y de la Ciudad Autónoma de Buenos Aires” (Art. 480 y 480 Bis de la Ley 5688). Esto a nuestro criterio es de una amplitud realmente intolerable. Esto así por que no se limita a determinar en que condiciones fácticas puede un juez solicitar se busque a una persona en el sistema. Es decir, si bien uno claramente podría ver los beneficios (por ejemplo, buscar a una persona desaparecida o en riesgo inminente), lo cierto es que también se puede utilizar para requerir, por ejemplo, la búsqueda de un testigo, o que se utilice el sistema para intentar determinar la dirección de algún individuo lo cual serían usos que deberían estar prohibidos por ley. En este sentido, se le otorga demasiadas

libertades a los jueces que son particularmente susceptibles a permitir a la Policía realizar sus investigaciones con muy pocos resguardos y que podrían eventualmente utilizar este Sistema de manera contraria a la Ley. En otro orden de ideas, piense V.S. que sucedería en el eventual caso que nuestras democracias por alguna u otra razón se desintegraran. El peligro de que un sistema de estas características exista en un contexto de persecución es realmente preocupante. Por ejemplo, ¿Qué hubiese sucedido en la última dictadura militar si los policías y jueces tuvieran la posibilidad de utilizar un sistema que le permitiría identificar a las personas en tiempo real en la calle? ¿Cuánta tanta otra gente habría sido secuestrada y desaparecida?

Volviendo al fallo de la Cámara de Apelaciones, otro elemento que se tomó como esencial para establecer la falta de base legal suficiente del sistema fue que el mismo no establece con exactitud a través de la ley que es lo que sucedería con los rasgos biométricos obtenidos de las imágenes de las Cámaras independientemente que las especificaciones técnicas del Sistema mencionaran que dichos registros biométricos se borrarían inmediatamente. En otras palabras, el SRF de la PSG no tendría una base legal suficiente por que no se establece por ley que es lo que tiene que suceder con los registros biométricos de las personas que son capturadas por las cámaras.

Notará V.S. que en el caso de SRFP de la CABA también existen las mismas deficiencias. La Ley 5688 lo único que establece es que las imágenes capturadas por el sistema de videovigilancia serán borradas a los 60 días de capturadas. Sin embargo, no hay ni un artículo que establezca que los registros biométricos obtenidos a través del procesamiento en vivo de las imágenes de las caras de aquellas personas que -como mis representados- transiten por las cámaras de la ciudad, vayan a efectivamente ser borrados inmediatamente.

Es precisamente por estos argumentos que la Cámara de Apelaciones entendió que el SRF de Gales era contrario a lo dispuesto por el Art. 8 de la CEDH y que no contaba con una base legal suficiente para poder limitar el derecho a la vida privada que aquél artículo establecía. De la misma manera esta parte entiende que V.S. podría utilizar argumentos muy similares a efectos de determinar la falta de adecuación de las normas atacadas con lo dispuesto por el CADH en su Art. 11.

E.2. La Evaluación de Impacto Ambiental y su falta de adecuación con la normativa local de Protección de Datos Personales

En segundo lugar, la Cámara de Apelaciones entendió que la Evaluación de Impacto en la Protección de Datos Personales realizada por la parte demandada era deficiente para cumplir con los propósitos dispuestos por la Ley de Protección de Datos Personales del Reino Unido (que es la adaptación del GDPR a la normativa interna) en su Art. 64 el cual reza:

“64. Evaluación de Impacto en los Datos Personales

(1) Donde algún tipo de procesamiento implique una probabilidad de alto riesgo a los derechos y libertades de los individuos, el controlador deberá, de manera previa al procesamiento, llevar a cabo una evaluación de impacto en la protección de datos personales.

(2) Una evaluación de impacto en los datos personales es una evaluación del impacto de una operación de procesamiento en la protección de los datos personales.

(3) Una evaluación de impacto en los datos personales deberá incluir lo siguiente:

(a) Una descripción general del procesamiento que se iría a realizar;

(b) Una evaluación de los riesgos a los derechos y libertades de los sujetos titulares de los datos personales a procesar.

(c) Las medidas que se piensan para mitigar esos riesgos;

(d) Medidas de seguridad y mecanismos que aseguren la protección de los datos personales para demostrar el cumplimiento de esta Parte, teniendo en consideración los derechos y legítimos intereses de los titulares de los datos y otras personas a las que les concierne el procesamiento.

(4) Al decidir si un tipo de procesamiento pueda implicar un alto riesgo a los derechos y libertades de los individuos, el controlador debe tener en consideración la naturaleza, el alcance, el contexto y la finalidad de ese procesamiento.”³⁶

³⁶ Esta es una traducción propia e informal de lo que dice dicho artículo en inglés: “64 Data protection impact assessment

(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.

(3) A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;

(b) an assessment of the risks to the rights and freedoms of data subjects;

(c) the measures envisaged to address those risks;

(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

En este apartado, la Cámara de Apelaciones determina que el demandado no realizó correctamente la Evaluación de Impacto ya que este habría establecido que el SRF no infringía lo dispuesto por el Art. 8 de la CEDH, cosa que, como surge del apartado inmediatamente anterior, la Cámara de Apelaciones había encontrado que no era cierto. El SRF viola el Art. 8 de la CEDH.

En el caso del SRFP de la CABA, resulta más que palmario que no existe en nuestra normativa de protección de datos (tanto local como nacional) una obligación expresa y legal que determine la obligatoriedad de la realización de una Evaluación de Impacto en la Protección de Datos (EIPD). Sin embargo, en lo que hace a la materia de protección de datos y conforme ya lo ha señalado la presentación de Amigo del Tribunal de la ATE, la EIPD si bien se ha incorporado recientemente como una obligación expresa en algunas legislaciones de Latinoamérica y Europa, resulta desde hace tiempo una buena práctica reconocida por normas técnicas internacionales.

Sin ir más lejos, nuestra propia Agencia de Acceso a la Información Pública (AAIP) ha sacado recientemente una “Guía de Evaluación de Impacto en Materia de Protección de Datos” junto a su par de la República Oriental del Uruguay.³⁷ En dicha Guía, entre otras cuestiones, se confirma la importancia de la realización de estas evaluaciones de impactos y las metodologías que se deben seguir para realizarlas.

Con esto esta parte quiere decir que una EIPD es completamente fundamental a efectos de entender los riesgos específicos a los derechos humanos de esta parte de la implementación del SRFP. Sin embargo, nada de esto se ha realizado. Nos encontramos ante una norma que sin siquiera analizar someramente las consecuencias de la implementación de una tecnología de este estilo, se ha implementado forzosamente y de manera contraria a las innumerables quejas de la sociedad civil y de ciudadanos preocupados como los de esta parte.

En este sentido, esta parte entiende que el hecho que el GCBA no haya realizado correctamente una EIPD es un elemento completamente contrario a la protección que nos otorga la CADH en su art. 11, el cual busca respetar la dignidad y la vida privada de las personas.

E. 3. Incumplimiento del deber de no discriminación

(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.”

³⁷ https://www.argentina.gob.ar/sites/default/files/guia_final.pdf

Finalmente, el último argumento utilizado a efectos de terminar por determinar la falta de adecuación convencional entre el SRF de la PSG y el Art. 8 de la CEDH fue que la PSG no estaba cumpliendo con el deber positivo que tiene el Sector Público de prevenir la discriminación indirecta. Cosa que no se realizó ya que no realizaron actos *ex ante* a los efectos de determinar de manera previa si la utilización del SRF tenía efectos discriminatorios o no.

Dicho esto V.S. me permito a su vez señalar el apartado D. de esta presentación donde se realiza el análisis de adecuación del SRFP de la CABA con las normas de no discriminación que rigen en el país y que deben ser respetadas.

E.4. Conclusión

Como podrá intuir V.S. este caso es importante por que es muy similar al caso de autos. No obstante, existen ciertas diferencias con las cuales V.S. deberá tener especial consideración ya que el fallo en cuestión de alguna u otra manera legitima el uso de el SRF siempre y cuando se cumplan con determinados requisitos. Para esta parte, no hay requisito alguno que este sistema cerrado pueda tener que legitime su uso. Es necesario también advertir que la historia del Reino Unido para con el derecho a la privacidad ha sido algo particular. En el famoso fallo *Malone v. Metropolitan Police Commissioner* del año 1979 en la High Court (Chancery Division), el juez Megarry dijo que en el Common Law inglés no existía un “derecho a la privacidad” y que por lo tanto el Gobierno podía tranquilamente intervenir los teléfonos de la parte actora sin orden de un juez. Esto demuestra que la actitud que ese país ha tenido con respecto al Derecho a la Privacidad ha sido, por lo menos, contenciosa. Y si a esto le sumamos lo que ha hecho el cuerpo de inteligencia británico (GCHQ) y sus campañas de vigilancia masiva, podremos entender por que existe un interés por parte de ese país de seguir construyendo y armando infraestructura que permita una vigilancia masiva. No obstante, aún así, el poder judicial de aquel país le puso un límite a este SRF.

En este orden de ideas, nuestra Constitución Nacional sí prevé la existencia de un Derecho a la Privacidad y vía el Art. 75 inc. 22, también incorpora los tratados internacionales que he mencionado y que prevén la existencia de un derecho a la vida privada cuya interpretación tiene que ser de las más amplias posibles. En este orden de ideas, no existe lugar alguno para que una herramienta de vigilancia masiva como el SRFP, que no tiene ni los más mínimos elementos de cuidado y precaución para con los derechos individuales de las personas. Más aún cuando hemos visto que lo hacen de manera completamente ilegítima y sin obtener el consentimiento de las personas que

transiten por las calles de la ciudad -como mis representados-. Es por esta razón que esta parte entiende que V.S. debería declarar la inconstitucionalidad de las normas atacadas y advertir que estas herramientas violan la CADH.

5. SOBRE LA MEDIDA CAUTELAR

En lo que hace a la solicitud de medida cautelar solicitada por la ONG que ha iniciado este expediente, esta parte, en razón de brevedad, hace propio los argumentos utilizados a efectos de que se otorgue y se suspendan los efectos que las normas atacadas tienen. Esto es de especial relevancia para mis representados ya que, de no acogerse la medida cautelar en cuestión, los mismos se encuentran expuestos a ser detenidos ilegalmente -así como le ha sucedido a otras personas que circularon por las calles de la ciudad-. En este sentido, la verosimilitud del derecho es bastante palmaria. Por un lado, mediante la utilización de este sistema se introduce un elemento que gatilla el poder punitivo restringiendo los derechos con los que cuentan mis representados de poder transitar por las calles de su ciudad sin el miedo que este SRFP los señale como culpables de delitos que jamás han cometido. Asimismo, también resulta bastante manifiesto la vulneración al régimen protectorio de sus datos personales, ya que, en contra de lo que dispone dicho régimen, no se está solicitando el consentimiento para realizar este tratamiento de datos complejo que implica el uso de este Sistema.

En otras palabras, aún si no se considerara que el SRFP representa una vulneración manifiesta a los derechos a la libertad ambulatoria, presunción de inocencia, y privacidad de mis representados, de todas maneras se muestra la total violación al régimen protectorio de datos personales que exige y establece un estándar de protección de estos derechos, que no están siendo respetados por este SRFP. En este sentido, es necesario recordar la máxima que establece que la apariencia o verosimilitud del derecho invocado por quien lo solicita (*fomus bonis iuris*) no exige un examen de certeza sobre la existencia del derecho pretendido, sino sólo su verosimilitud. En otras palabras, no se debe exigir del peticionario que provea absolutamente todas las pruebas que permitan determinar “la verdad jurídica objetiva” ya desde la presentación del libelo de demanda. Sencillamente es necesario aportar la suficiente evidencia -que esta parte cree que ha aportado- de la verosimilitud de los derechos en juego y la importancia que estos tienen para mis representados.

En otro orden de ideas, el peligro en la demora también queda claramente comprobado ya que la violación que genera el SRFP y las normas que lo sostienen, es sostenida y permanente en el tiempo. Esto así por que alteran los derechos de mis representados de poder transitar por las calles siendo completamente anónimos y sin tener miedo de ser detenidos por la policía. Recordemos V.S. que es el propio GCBA es el que ha provisto información que demuestra, sin lugar a dudas e interpretaciones, la falta total y absoluta de eficiencia del sistema. Es decir, el SRFP no es exacto, está plagado de errores y potencialmente discriminador. El mero hecho que este SRFP se encuentre funcionando, o que se encuentre “legitimado” por la aprobación de una ley que fue aprobada sin apoyo de la oposición en el recinto de la legislatura, no quita que su uso no atente contra los derechos de mis representados. Ellos tienen derecho a transitar por las calles de la ciudad sin tener miedos o preocupaciones de ser potencialmente detenidos y puestos a disposición de la justicia sin haber realizado ningún delito. Nadie en este mundo, tiene derecho a exigirles documentación sin que exista un justificativo. El levantamiento de una alarma de este sistema NO ES UN JUSTIFICATIVO. Es necesario recordar que el peligro en la demora (*periculum in mora*), es aquel recaudo que exige la probabilidad de que la tutela jurídica definitiva que la demandada aguarda de la sentencia a pronunciarse en el proceso principal no pueda en los hechos realizarse, es decir que, a raíz del transcurso del tiempo, se ponga en peligro la validez de dicha sentencia.

En efecto, si V.S. no otorgara dicha medida cautelar, mis representados podrían eventualmente ser detenidos por un mal funcionamiento de este sistema. Y, si esto sucediera, el presente proceso devendría en abstracto para ellos por que el miedo que ha motivado la interposición de este reclamo se concretaría.

Asimismo, también es necesario puntualizar que gran parte del peligro en la demora también deriva del hecho que este sistema extrae rasgos biométricos que son datos sensibles de mis representados. En este sentido, esta extracción sin consentimiento de ellos, es completamente ilegal e ilegítima. Seguramente esta extracción ya se ha realizado ya que mis representados son ciudadanos de esta ciudad y mientras el ASPO no les sea aplicable a ellos, han tenido que circular por la ciudad con el consecuente riesgo de que estos datos sensibles se extraigan de ellos sin su autorización expresa.

Es por todas estas razones que esta parte entiende que V.S. debería admitir la medida cautelar de manera inmediata e inaudita parte.

6. PLANTEA CASO FEDERAL

Se formula expreso planteo del caso federal para el supuesto improbable de que las instancias ordinarias no acogieran la acción deducida formal o sustancialmente, conforme a las prescripciones del artículo 14 de la Ley 48, a fin de articular oportunamente el recurso extraordinario ante la Corte Suprema de Justicia de la Nación, por violación de los preceptos constitucionales individualizados en esta presentación.

7. PRUEBA

Ofrezco como prueba del derecho de mi parte la siguiente:

Documental:

- 1) Anexo I: NO-2019-33745359-GCABA-DGEYTI
- 2) Anexo II: NO-2019-25581723-GCABA-DGEYTI
- 3) Anexo III: Convenio de RENAPER y Ministerio
- 4) Anexo IV: NO-2019-37063734-GCABA-DGEYTI
- 5) Anexo V: Notas de prensa varias linkeadas en la presente presentación.
- 6) Anexo VI: DNI de los Actores

Informativa:

En el supuesto e hipotético caso que la parte demandada no reconozca los hechos expuestos y descriptos anteriormente, y que desconozca la documental acompañada solicito se libre oficio a la Sala III de la Cámara de Apelaciones en lo Contencioso Administrativo y/o el Juzgado Contencioso Administrativo y Tributario N° 23, Secretaría N° 45, a efectos de que:

- 1) Se remita el Expediente 9480/2019-0 donde obran los documentos acompañados al presente como Anexo I, Anexo II, Anexo III y Anexo IV, así como otra evidencia que demuestra la inconstitucionalidad del SRFP en cuestión.

Pericial

Por el otro lado, si bien a esta parte no se le escapa lo dispuesto por el Art. 9 de la Ley de Amparo en cuanto a que la *“La prueba pericial sólo será admisible*

en forma excepcional cuando las circunstancias del caso lo justifiquen a fin de dictar sentencia y siempre que su producción sea compatible con la naturaleza sumarásima de la acción de amparo.”, lo cierto es que el presente proceso, en virtud de sus particularidades técnicas, parecería ser un caso excepcional que admitiría la realización de esta prueba. Por esta razón, solicito se sortee un Perito Informático quién deberá contestar las siguientes preguntas con las constancias del presente expediente, los enlaces y videos señalados y mencionados, así como teniendo toda la prueba solicitada por todas las partes:

1) ¿Desde cuándo se ha puesto en marcha este Sistema de Reconocimiento Facial de Prófugos?

2) ¿Cómo funciona este SRFP?

3) ¿A dónde van a parar los datos extraídos por las cámaras?

4) ¿Cuáles son los resguardos que se tienen y se deberían tener de los datos extraídos por las cámaras?

5) ¿Qué es un dato biométrico?

6) ¿El SRFP hace tratamiento de datos biométricos?

7) ¿Por qué es importante cuidar adecuadamente los datos biométricos extraídos por estas cámaras?

8) ¿Es el sistema de cifrado 3DES un sistema de cifrado adecuado para el resguardo de la información?

9) ¿Puede el Sistema determinar sobre que caras extraer rasgos biométricos y sobre cuáles no?

10) ¿Entiende usted que un sistema de estas características puede ser potencialmente discriminatorio? ¿Por qué?

11) ¿Qué es y cómo funciona el “sistema forense” y “sistema predictivo”?

Testimonial

Solicito se cite a prestar declaración testimonial a la Sra. Cecilia Inés Amigo que es Coordinadora del Plan Integral de Videovigilancia en el Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires, de acuerdo al interrogatorio que oportunamente se acompañará según art. 429 C.P.C.C.N, y quien declarará sobre aspectos relativos al funcionamiento del SRFP, a las condiciones en las cuales el mismo se encuentra actualmente y a los compromisos a los cuales se ha comprometido la empresa licenciataria.

Nombre: Cecilia Inés Amigo

DNI: 33420123

Profesión: Coordinadora del Plan Integral de Videovigilancia en Ministerio de Justicia y Seguridad (C.A.B.A)

Domicilio: Cerrito 236, Piso 3° (1010) – Capital Federal

Domicilio alternativo: Alvear 3322 (1824) – Lanus – Provincia de Buenos Aires.

En el eventual caso que no se encuentre en ninguno de esos dos domicilios solicito se envíe un oficio al RENAPER para que le remita a V.S. el domicilio en cuestión para poder ser notificada y llamada a brindar declaración testimonial.

8. PETITORIO

Por lo expuesto anteriormente le solicito a V.S. que:

- 1) Me tenga por presentado, por parte en el carácter invocado y por constituido el domicilio procesal indicado.
- 2) Se tenga presente la prueba ofrecida.
- 3) Se tenga por planteado el caso federal
- 4) Oportunamente se dicte sentencia favorable a mi parte con expresa imposición de costas a la parte contraria.

Proveer de conformidad que,

SERÁ JUSTICIA



VICTOR ALBA CASTELLANO
Abogado
C.P.A.C.P. Nº 123 - Pº 482

ANEXO I



GOBIERNO DE LA CIUDAD DE BUENOS AIRES
"2019 -Año del 25° Aniversario del reconocimiento de la autonomía de la Ciudad de Buenos Aires"

Número:

Buenos Aires,

Referencia: s/ "O.D.I.A. c/ G.C.B.A. s/ Amparo", Expte. N° 9480/19

En respuesta a: NO-2019-33610651-GCABA-DGALSE

A: Fabiana Costanza (DGALSE),

Con Copia A: NATALIA TANNO (DGAYCSE), Gustavo Roldan (DGEYTI),

De mi mayor consideración:

Tengo el agrado de dirigirme a Ud., en relación al pedido de información efectuado en el marco de los autos caratulados "O.D.I.A. c/ G.C.B.A. s/ Amparo", Expte. N° 9480/19, en trámite por ante el Juzgado de Primera Instancia en lo Contencioso, Administrativo y Tributario N° 23, Secretaría N° 45,

Atento a ello, se dará respuesta a aquellos requerimientos que resulten compatibles con la competencia de la Dirección General a mi cargo.

10) ¿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?

El Centro de Monitoreo Urbano (CMU) cuenta con un Protocolo de actuación sobre el Procedimiento en caso de alerta arrojada por el "Sistema de Reconocimiento Facial de Prófuagos".

Asimismo cuenta con un Convenio de Confidencialidad utilizado para la totalidad del personal del Centro de Monitoreo Urbano de acuerdo a lo normado en el artículo 483 de la Ley N° 5.688/16.

Por último, el CMU implementó la gestión de seguimiento de calidad respecto al sistema de reconocimiento facial de prófuagos.

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

La auditoria del funcionamiento del Sistema de Reconocimiento Facial de Prófuagos es llevada a cabo por la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires. El sistema de referencia no almacena imágenes a excepción de las alertas correspondiente a aquellas personas buscadas por la justicia. Conforme a lo enunciado, las imágenes que no deviene en una alerta positiva son automáticamente descartadas del proceso de almacenamiento del sistema.

15) 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?

Se utiliza un cifrado 3 DES. Se ha establecido en el art. 2 del Anexo de la Resolución 398/19 que “[...] El Sistema de Reconocimiento Facial de Prófugos será empleado únicamente para tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial de la Nación, Provincial y de la Ciudad Autónoma de Buenos Aires como así también para detección de personas buscadas exclusivamente por orden judicial, registradas en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC). Salvo orden judicial, se encuentra prohibido incorporar imágenes y registros de otras personas que no se encuentren registradas en el CONARC”.

Por lo tanto, solicitamos se nos de la siguiente información:

21) Informe si el software reconoce a menores de edad

NO. Dado que en la base de datos del CONARC no posee datos respecto a menores de edad. Se enfatiza que dicha base contiene registros de personas con órdenes de restricción de la libertad impartidos por la justicia y/o rebeldías.

22) ¿Qué información se registra y archiva acerca de ellos?

No se archivan registros por lo mencionado en el punto anterior.

23) ¿Con quién se comparte dicha información y con qué fines?

No existe información que se comparta.

29) ¿Cuántos individuos en total han sido autorizadas para tener acceso y poder operar este sistema?

En total existen 114 usuarios.

22 corresponden a personal de gestión operativa (área técnica) quienes pueden generar usuarios exclusivamente.

77 usuarios finales del sistema que solo pueden visualizar y recibir alertas (operadores, personal del CMU y personal del Ministerio).

15 usuarios con el perfil PFA Retiro.

30) ¿Cuántos civiles han sido autorizados por el Ministerio de Justicia y Seguridad?

Los usuarios autorizados en la sala de monitoreo son 20, quienes se encuentran secundados bajo la supervisión del personal policial.

31) De existir civiles autorizados, ¿Qué rol cumplen en la operatoria del Sistema y por qué es necesario que estos tengan acceso?

Porque el personal civil se encuentra a cargo de la visualización de las cámaras asignadas por puesto de monitoreo y es secundado bajo la supervisión del personal policial presente en la sala.

Además de los puntos requeridos anteriormente, lo cierto es que, a través de este sistema se ponen en peligro diversos derechos civiles (ej. Libertad ambulatoria, privacidad, autodeterminación informativa, etc) de las personas. Si no se tiene un buen control que limiten las posibilidades de abuso, estos derechos pueden ser afectados innecesariamente. Por esta razón, solicitamos se nos indique si ante una alerta levantada por el sistema:

37) ¿Se le comunica al presunto prófugo por qué motivo se lo está demorando, así como en qué causa y en qué juzgado radica la misma? ¿En qué momento?

El personal de facción una vez que identifica a la persona le explica que saltó un alerta en el Sistema de Reconocimiento Facial de Prófugos al Centro de Monitoreo Urbano, le informa en el marco de que causa, el delito que se le imputa y procede a notificarlo en el mismo acto.

38) ¿Se realiza un seguimiento del presunto prófugo una vez puesto a disposición de la justicia?

No, el MJyS no es órgano competente para realizar seguimiento de presuntos prófugos. La Policía de la Ciudad, en su carácter de auxiliar de la justicia, lo pone a disposición de esta.

39) ¿Qué sucede si la persona a quien se demora no tiene su DNI o no posee documentación que lo identifique?

Si no tiene DNI, se le solicita Cédula o Pasaporte (Ver Ley N° 23.950). El personal de facción cuenta con el sistema *morpho touch*. Este es un novedoso sistema de última generación que permite al personal policial verificar en segundos si pesa sobre la persona demorada pedidos de captura.

40) Ante un caso de “falso positivo” ¿cómo es el protocolo que los agentes que realizaron la detención deben seguir?

El personal policial deja asentado en un acta los datos de la persona demorada y se la invita a que siga circulando.

41) El reporte de una alerta del sistema, por si sola, ¿es una circunstancia que justifica la detención o demora de una persona?

Si porque los datos que saltan en la alerta provienen de la base de datos del CONARC en el cual se cargan todas las causas en las que las personas tienen pedidos de capturas o se encuentran estado de rebeldía.

42) ¿En qué momento se le notifica al Juez/Fiscal correspondiente que ha habido una alerta en el Sistema de Reconocimiento Facial de Prófugos?

Inmediatamente.

44) ¿En qué tipo de aparatos reciben las alertas generadas por el sistema los agentes de la Policía?

Teléfono institucional (POC), mediante el cual el personal policial efectúa comunicaciones respecto a necesidades operativas. Las alertas son recibidas únicamente en los teléfonos asignados a los efectivos abocados a dicha tarea. La tecnología de estos dispositivos son Smartphone con tecnología 4G, sistema Androide, marca Samsung.

¿En qué momentos los agentes destruyen aquellos archivos que le fueron enviados a esos aparatos?

Los teléfonos institucionales no almacenan eventos.

¿Qué sistema o protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos y como se audita su correcta destrucción?

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

Las alerta llegan a los efectivos asignados a dicha función mediante una APP (aplicación) específica de desarrollo propio, la cual posee normas de seguridad y uso (control de logging, y marca de agua en usuarios).

46) ¿Qué policías reciben esta información?

Esta Información es recibida por personal del Centro de Monitoreo Urbano y personal policial asignado al servicio del Sistema de Reconocimiento Facial de Prófugos.

47) ¿cuántos agentes reciben esta información?

El personal abocado por turno al servicio específico.

48) ¿En qué consisten estas alertas?

Los mismos reciben alertas del sistema de Reconocimiento Facial de Prófugos respecto a personas con pedidos de captura o en estado de rebeldía existentes en la base de datos del CONARC

50) ¿Cuántas personas han sido detenidas o demoradas al día de la fecha con causa en el levantamiento de una alerta por el sistema de reconocimiento facial?

El total de personas identificadas puestas a disposición de la Justicia fueron 1.337 hasta el 25 de julio del corriente año. A la actualidad, 1648 personas han sido puestas a disposición de la justicia.

51) ¿Cuántas veces no se ha correspondido la persona buscada con la persona demorada? Es decir, ¿cuántos “falsos positivos” han ocurrido desde la implementación del Sistema de Reconocimiento Facial de Prófugos?

Un total de 123 falsos positivos hasta el 25 de julio del corriente año. A la actualidad, 141 falsos positivos.

52) ¿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 Resolución 1068 - E/2016.

El MJyS no es órgano competente para conceptuar o definir los delitos graves.

53) 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”?

A la actualidad, 1648 personas han sido identificadas y puestas a disposición de la justicia.

Ha trascendido al Público que la empresa contratada a efectos de realizar el desarrollo de este Sistema es la empresa DANAIDE SA. En consideración de que el software se ha adquirido por contratación directa –según consta en la página web del GCBA-, que el pliego de especificaciones técnicas fue publicado el 3 de abril de 2019 y se implementó días después solicitamos se nos informe:

54) Se justifica la adjudicación por contratación directa a DANAIDE S.A. en virtud de lo dispuesto por el Art. 28 inc. 6 de la Ley de Compras y Contrataciones de la Ciudad Autónoma de Buenos Aires. Por lo tanto, ¿El sistema de Video Vigilancia de la CABA fue íntegramente confeccionado por esta firma? De no ser así, ¿por qué no se realizó una Licitación Pública?

Si, el sistema de videovigilancia ha sido confeccionado íntegramente por la contratista de referencia.

59) Ante una vulnerabilidad del sistema de Reconocimiento Facial o un ataque informático donde se expongan los datos y/o archivos de los ciudadanos generados por este sistema ¿Existe un sistema de crisis que incluya notificar a los ciudadanos de esta exposición?

La única información relevante almacenada en estos servidores es la obtenida del CONARC, base publica a la cual puede acceder cualquier ciudadano; por tal motivo no se considera necesario ningún sistema de crisis si es que se diera el caso de acceso a la base sin autorización.

60) ¿Qué compromiso tuvo la empresa respecto a la cantidad posible de falsos positivos que su sistema podía generar?

Se ratifica lo informado oportunamente, en cuanto a que el índice de precisión es superior al 95% conforme a lo enunciado en el pliego técnico del oferente.

61) ¿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?

Se realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los casos los porcentajes de error exigidos

62) ¿Qué datasets fueron utilizados para ese entrenamiento y que organismo fue responsable?

Primera parte ídem, resp. N° 61. El organismo responsable fue el Ministerio de Justicia y Seguridad.

63) ¿A qué porcentaje de confiabilidad en una coincidencia se ha comprometido la empresa? ¿A qué porcentaje de efectividad respecto del sistema completo se ha comprometido la empresa?

El porcentaje es +78 % (según manual de uso), hoy calibrado en + 80 %.

64) ¿Quién es el responsable del control y seguimiento acerca de los compromisos asumidos por la empresa?

La Secretaria de Administración de Seguridad y Emergencias.

65) ¿Qué seguimiento y control respecto de los compromisos asumidos por la empresa se llevarán a cabo?

El proceso de control y seguimiento contempla: análisis detallado de los falsos positivos para que los mismos se encuentre dentro de los parámetros ofertados,

disponibilidad del servicio, proceso de instalaciones y calibración de cámaras, auditoria de base de datos de prófugos, gerenciamiento de la infraestructura física del sistema, análisis de SLA (acuerdo de nivel de servicio) ante fallas del sistema y optimizaciones permanentes del software conforme a los requerimientos técnicos y operativos del MJyS.

67) ¿Se ha hecho una auditoría del software por un tercero independiente?

Conforme a la Resolución 398/2019, se invita a la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires a auditar el funcionamiento del Sistema de Reconocimiento Facial de Prófundos.

68) Se solicita se nos brinde el código fuente del software en soporte digital y enviado al correo electrónico que se señala en el encabezado.

No se tiene acceso a esta información, por corresponder al secreto comercial de la empresa, que posee el copyright de la licencia del mismo.

Asimismo, se han detectado ciertas expresiones en el llamado “Pliego de Especificaciones Técnicas del Servicio de Análisis Integral de Video” obscuras y poco claras que a continuación señalaremos y sobre las cuales solicitamos cierta información:

Con respecto al Punto 1. (Objeto):

76) “[...] Dicho servicio tendrá como objetivo el análisis integral en tiempo real sobre imágenes de video en vivo para la detección facial de personas buscadas basada en bases de datos de imágenes de rostros y de análisis integral de video para la detección de diferentes patrones de comportamiento y cambios de condiciones ambientales. El servicio será prestado sobre todas las cámaras de video vigilancia que técnicamente lo permitan, como así también a las imágenes almacenadas en los sistemas de resguardo de imágenes, al momento de la presentación de su oferta. [...]” “[...] Las imágenes captadas que generen algún tipo de alerta como toda la información vinculada a la misma, deberán ser guardada de forma encriptada para futuros análisis [...]” “[...] Contar con una base de datos fotográfica de hasta cien mil (100.000) rostros para su posterior identificación formando una lista negra de personas buscadas. [...]”(El destacado es nuestro).

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?

n. ¿Quién tiene permiso para modificar esta lista? ¿Qué parámetros o requisitos pide el sistema a efectos de modificar la lista?

Apartados A/B/E: en los que se requiere se indique "que se quiso decir" con: "detección de diferentes patrones de comportamiento" y "cambios de condiciones ambientales", y en qué consisten los "futuros análisis" que se mencionan. Al respecto, se estima que todas esas expresiones resultan suficientemente claras para entender su significado literal, excediendo el objeto de la ley 104 expedirse acerca de otras interpretaciones que puedan darse a las mismas.

Apartados J/K/L/M/N: Conforme surge del propio texto del pliego técnico, la lista negra es una denominación de la base de datos de personas prófugas de la justicia. Por lo cual, las preguntas enunciadas ya han sido contestadas con anterioridad.

Para más información ver:

<https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83/5qmQHYdlWCoEzPIKU0JAvRZ7kltC74K/7Tw11ctBR9dfFZZemaLoi969Lwy2BFPNwVGFQ7XOHCTEKW51rAObrIXsdfYAs0SFw==>

En el mismo pliego se han hecho una serie de manifestaciones genéricas que, dado el efecto que la interpretación que las mismas tendrían en los derechos fundamentales de las personas, hacen de suma importancia que se aclare. Así, se ha establecido los siguientes requisitos:

77) "[...] Ante eventos repetitivos, el sistema deberá enmascarar automáticamente dichos eventos a modo de optimizar la visualización de los operadores y proveer de información de notificaciones eficientemente. [...]" "[...] El sistema deberá considerar áreas de enmascaramiento tanto dentro como fuera de la zona de detección para así evitar falsos positivos. [...]" "[...] El sistema deberá tener una historia de los eventos con toda la información necesaria para su comprensión: imagen y posibilidad de reproducción de la grabación alrededor del tiempo en que el evento ocurrió. [...]" "[...] El sistema deberá tener la capacidad de purga periódica de datos acumulados, considerando su antigüedad. [...]" "[...] El sistema deberá considerar dos (2) niveles de permisos: uno limitado a la visualización de datos y otro con disponibilidad para todas las operaciones. [...]" "[...] El sistema no deberá superar la detección de falsos positivos en un 15% del total de los eventos detectados. [...]" "[...] Persona que cruza una línea [...]" "[...] Persona moviéndose en un área: ante la detección de una persona en una zona estéril definida previamente. [...]" "[...] Hacinamiento: alerta por la detección de una cierta cantidad de personas detectadas durante una cierta cantidad de tiempo. [...]" "[...] Acercamiento entre personas: alerta ante la detección de un cruce de línea de una segunda persona en un tiempo menor al definido en la regla. [...]" "[...] Merodeo: alerta por personas residiendo en una zona durante un tiempo mínimo definido y comportándose de una manera sospechosa que respalde la credibilidad de que su objetivo es una actividad delictiva. [...]" "[...] Ocupación: alerta ante la detección de un límite de personas definidas para un área. [...]" "[...] El sistema deberá permitir configurar una tolerancia sobre las búsquedas, permitiendo y aceptando posibles falsos positivos para la obtención de información. [...]" "[...] A su vez, deberá permitir la detección de la emoción del rostro (feliz, sorprendido, neutral, triste, miedo, enojo y disgusto). [...]" "[...] Deberá permitir la indexación masiva de datos de video, registrando la información de todas las personas que aparecen, permitiendo una búsqueda dinámica y veloz de las personas de interés. [...]" (El destacado es nuestro).

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?

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?
- q. ¿Con que sin 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”?

Lo enunciado en los párrafos previos, no corresponden a características técnicas del Sistema de Reconocimiento Facial de Prófugos. Estos conceptos devienen de la adquisición de otros software (predictivo y forense).

Ver:

<https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83|5qmQHYdlWCoEzPIKU0JAvRZ7kltC74K|7Tw11ctBR9dfFZZemaLoi969Lwy2BFPNwVGFQ7XOHCTEKW51rAObrIXsdfYAs0SFw==>

Sin otro particular saluda atte.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.10.30 15:35:28 -03'00'

Digitally signed by Comunicaciones
Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.10.30 15:35:29 -03'00'

ANEXO II



GOBIERNO DE LA CIUDAD DE BUENOS AIRES
"2019 -Año del 25° Aniversario del reconocimiento de la autonomía de la Ciudad de Buenos Aires"

Número:

Buenos Aires,

Referencia: s/ URGENTE Y PREFERENCIAL DESPACHO - LEY 104 - Expediente N° 2019-21385378- GCABA-DGSOCAI

En respuesta a: NO-2019-25526527-GCABA-DGALSE

A: Fabiana Costanza (DGALSE), Gustavo Roldan (DGEYTI),

Con Copia A:

De mi mayor consideración:

Tengo el agrado de dirigirme a Ud. en relación al requerimiento efectuado a través de la Ley 104 "Acceso a la Información", en el marco de la cual se solicita, la información que a continuación se detalla y esta dentro del marco de mi competencia:

1) ¿Cuántas cámaras de monitoreo posee la CABA?

El Centro de Monitoreo Urbano (CMU) cuenta con un total de 7.970 cámaras de video vigilancia (6.544 instaladas en superficie - espacio público, 739 en Subterráneo y 687 de proceso de integración con AUSA, SBASE, Tránsito, Anillo Digital, etc.).

2) ¿Cuántas de ellas están habilitadas para utilizar este "Sistema de Reconocimiento Facial de Prófugos"?

La totalidad de las cámaras correspondientes al MJyS poseen la tecnología necesaria para la implementación de licencias de reconocimiento facial.

3) ¿Cuál es la ubicación exacta de aquellas cámaras que estarán utilizando este nuevo "Sistema de Reconocimiento Facial de Prófugos"?

Las ubicaciones de uso e implementación de las licencias de referencia se establecen conforme a los requerimientos de seguridad y operatividad policial.

4) ¿En qué resolución de video capturan las imágenes estas cámaras?

Resolución 4k

5) ¿Dónde se encuentra ubicado el Centro de Monitoreo Urbano (de ahora en más "CMU") que haría el procesamiento de las imágenes?

Av. Guzmán 396, Chacarita, CABA (Comuna 15).

6) ¿Cuál fue el costo de la construcción de la infraestructura necesaria para transmitir dichos videos al CMU?

La infraestructura utilizada para la transmisión de imágenes de video al CMU es la ya implementada para el Plan Integral de Videovigilancia. Por lo que no se detentan costos de arquitectura técnica adicionales para la transmisión de imágenes de las ya existentes.

7) ¿Qué formato de video se utiliza para la captura de las imágenes? ¿son las imágenes sometidas a compresión? ¿Qué método de compresión y descompresión es utilizada? ¿Qué ancho de banda es necesario para la transmisión de las imágenes desde cada cámara al CMU?

El formato es Mpeg-4. Las imágenes son sometidas a un proceso de compresión, cuyo método es H.264/H.265. El ancho de banda utilizado para la transmisión de imágenes de video de licencias de reconocimiento facial es de hasta 8 megas.

8) ¿Se utiliza algún sistema de cifrado para la transmisión de la información desde la captura realizada por las Cámaras hasta el CMU? De ser así, ¿qué sistema de cifrado es utilizado?

El cifrado es Ipsec.

9) ¿Qué tipo de infraestructura tuvo que ser implementada para la realización de dicho procesamiento y para la transmisión de las imágenes?

Se puso en funcionamiento una granja de servidores para procesamiento de imágenes.

11) ¿De qué manera se procesan las imágenes que son capturadas por las cámaras?

Se efectúa una comparación de la imagen capturada por la cámara con la imagen que la persona que figura en la lista del CONARC posee en el RENAPER.

12) ¿Durante cuánto tiempo son almacenadas las imágenes capturadas por las cámaras y que son procesadas a través del “Sistema de Reconocimiento Facial de Prófugos”?

Las imágenes capturadas por el Sistema de Reconocimiento Facial no son almacenadas, excepto las de alertas positivas de acuerdo a lo estipulado en el artículo 484 de la Ley N° 5.688/16 (B.O. N° 5030 de fecha 21/12/2016) y Decreto reglamentario N° 312-MJYSGC/18 (B.O. N° 5464 de fecha 25/9/2018).

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

La auditoría del funcionamiento del Sistema de Reconocimiento Facial de Prófugos es llevada a cabo por la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.

14) ¿Dónde se realiza físicamente el emparejamiento o la coincidencia de los puntos de los rostros capturados por las cámaras con los puntos de los rostros capturados de la base de datos utilizada para realizar dicho procesamiento?

En DataCenter del MJyS.

15) 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?

Por una cuestión de seguridad informática, no es posible brindar esta información.

21) Informe si el software reconoce a menores de edad

NO.

22) ¿Qué información se registra y archiva acerca de ellos?

N/A

23) ¿Con quién se comparte dicha información y con qué fines?

N/A

24) ¿Existe algún convenio realizado entre el CONARC y el RENAPER para la transmisión de los datos biométricos?

Con en el RENAPER, la base del CONARC es publica <https://servicios.dnrec.jus.gov.ar/CONARCPublico/>

43) Una vez realizada la detención y cumplida la orden judicial de captura, ¿En qué momento se destruyen los datos y archivos generados por el sistema?

Cuando se produce una detención dando cumplimiento a la orden judicial de captura, las imágenes se ponen a disposición de la justicia si es que son requeridas, caso contrario el sistema las destruye de forma automática en el plazo de 60 días corridos desde su captación.

44) ¿En qué tipo de aparatos reciben las alertas generadas por el sistema los agentes de la Policía?

Teléfono institucional (POC) –

¿En qué momentos los agentes destruyen aquellos archivos que le fueron enviados a esos aparatos?

Los POC no almacenan eventos

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

A través de una APK específica de desarrollo propio. Información respecto a la captura de la persona proporcionada por el CONARC.

49) ¿Cuántas alertas ha disparado el sistema desde su implementación y puesta en funcionamiento?

Alertas arrojadas 3059.

55) ¿Cuánto tiempo se tuvo para la instalación de este nuevo sistema de reconocimiento facial?

El proceso de instalación del sistema de reconocimiento facial de prófugos y puesta a punto del mismo fue de 4 meses (incluye periodo de testing).

56) ¿Hubo período de prueba antes de la puesta en funcionamiento de este sistema? ¿cuándo se ha firmado el acta de entrega definitiva de obra correspondiente a la contratación de todo sistema informático?

Si, se realizaron pruebas sobre muestras testigos seleccionadas para tal fin. El acta de entrega definitiva del sistema se realizó el 23/04.

59) Ante una vulnerabilidad del sistema de Reconocimiento Facial o un ataque informático donde se expongan los datos y/o archivos de los ciudadanos generados por este sistema ¿Existe un sistema de crisis que incluya notificar a los ciudadanos de esta exposición?

El DataCenter del Ministerio es de características TIER II, los datos de las personas son de prófugos de la justicia, información suministrada por el CONARC

60) ¿Qué compromiso tuvo la empresa respecto a la cantidad posible de falsos positivos que su sistema podía generar?

El índice de precisión es superior al 95% conforme a lo enunciado en el pliego técnico del oferente.

61) ¿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?

Esta información corresponde al desarrollo del producto y es un detalle que posee el copyright de la licencia del mismo, por lo cual no se posee acceso a esta información.

62) ¿Qué datasets fueron utilizados para ese entrenamiento y que organismo fue responsable?

Ver respuesta 61.

63) ¿A qué porcentaje de confiabilidad en una coincidencia se ha comprometido la empresa? ¿A qué porcentaje de efectividad respecto del sistema completo se ha comprometido la empresa?

El porcentaje es +78 % (según manual de uso), hoy calibrado en + 80 %.

65) ¿Qué seguimiento y control respecto de los compromisos asumidos por la empresa se llevarán a cabo?

El proceso de control y seguimiento contempla: análisis detallado de los falsos positivos para que los mismos se encuentre dentro de los parámetros ofertados, disponibilidad del servicio, proceso de instalaciones y calibración de cámaras, auditoria de base de datos de prófugos, gerenciamiento de la infraestructura física del sistema, análisis de SLA ante fallas del sistema, etc.

66) ¿Existe alguna instancia, en cualquier parte de todo el sistema (software o hardware), en el que el resultado de uno o más procesos del mismo sea utilizado como retroalimentación o input para entrenar o modificar el mecanismo de reconocimiento facial de cualquier forma?

No.

67) ¿Se ha hecho una auditoría del software por un tercero independiente?

Conforme la Resolución 398/2019, la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires es el organismo auditor

68) Se solicita se nos brinde el código fuente del software en soporte digital y enviado al correo electrónico que se señala en el encabezado.

Ver respuesta 61.

74) Copia del convenio realizado entre el Gobierno de la Ciudad de Buenos Aires y el CONARC para el envío de las imágenes, archivos, e informaciones correspondientes y relacionadas a este Sistema de Reconocimiento Facial.

Ver pregunta 24

76) “[...] Dicho servicio tendrá como objetivo el análisis integral en tiempo real sobre imágenes de video en vivo para la detección facial de personas buscadas basada en bases de datos de imágenes de rostros y de análisis integral de video para la detección de diferentes patrones de comportamiento y cambios de condiciones ambientales. El servicio será prestado sobre todas las cámaras de video vigilancia que técnicamente lo permitan, como así también a las imágenes almacenadas en los sistemas de resguardo de imágenes, al momento de la presentación de su oferta. [...]” “[...] Las imágenes captadas que generen algún tipo de alerta como toda la información vinculada a la misma, deberán ser guardada de forma encriptada para futuros análisis [...]” “[...] Contar con una base de datos fotográfica de hasta cien mil (100.000) rostros para su posterior identificación formando una lista negra de personas buscadas. [...]”(El destacado es nuestro).

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?

n. ¿Quién tiene permiso para modificar esta lista? ¿Qué parámetros o requisitos pide el sistema a efectos de modificar la lista?

<https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83j5qmQHYdlWCoEzPIKU0JAvRZ7klC74K/7Tw1lctBR9dfFZZZemaLoi969Lwy2BFPNwVGFQ7XOHCTEKW51rAOObRIXsdfYAs0SFw==>

77) “[...] Ante eventos repetitivos, el sistema deberá enmascarar automáticamente dichos eventos a modo de optimizar la visualización de los operadores y proveer de información de notificaciones eficientemente. [...]” “[...] El sistema deberá considerar áreas de enmascaramiento tanto dentro como fuera de la zona de detección para así evitar falsos positivos. [...]” “[...] El sistema deberá tener una historia de los eventos con toda la información necesaria para su comprensión: imagen y posibilidad de reproducción de la grabación alrededor del tiempo en que el evento ocurrió. [...]” “[...] El sistema deberá tener la capacidad de purga periódica de datos acumulados, considerando su antigüedad. [...]” “[...] El sistema deberá considerar dos (2) niveles de permisos: uno limitado a la visualización de datos y otro con disponibilidad para todas las operaciones. [...]” “[...] El sistema no deberá superar la detección de falsos positivos en un 15% del total de los eventos detectados. [...]” “[...] Persona que cruza una línea [...]” “[...] Persona moviéndose en un área: ante la detección de una persona en una zona estéril definida previamente. [...]” “[...] Hacinamiento: alerta por la detección de una cierta cantidad de personas detectadas durante una cierta cantidad de tiempo. [...]” “[...] Acercamiento entre personas: alerta ante la detección de un cruce de línea de una segunda persona en un tiempo menor al definido en la regla. [...]” “[...] Merodeo: alerta por personas residiendo en una zona durante un tiempo mínimo definido y comportándose de una manera sospechosa que respalde la credibilidad de que su objetivo es una actividad delictiva. [...]” “[...] Ocupación: alerta ante la detección de un límite de personas definidas para un área. [...]” “[...] El sistema deberá permitir configurar una tolerancia sobre las búsquedas, permitiendo y aceptando posibles falsos positivos para la obtención de información. [...]” “[...] A su vez, deberá permitir la detección de la emoción del rostro (feliz, sorprendido, neutral, triste, miedo, enojo y disgusto). [...]” “[...] Deberá permitir la indexación masiva de datos de video, registrando la información de todas las personas que aparecen, permitiendo una búsqueda dinámica y veloz de las personas de interés. [...]” (El destacado es nuestro).

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?

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?
- q. ¿Con que sin 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”?

<https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83|5qmQHYdlWCoEzPIKU0JAvRZ7klC74K|7Tw1|ctBR9dfFZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObRlXsdfYAs0SFw==>

Sin otro particular saluda atte.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.08.15 17:40:11 -03'00'

Digitally signed by Comunicaciones
Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.08.15 17:40:11 -03'00'

ANEXO

III

**CONVENIO DE COOPERACIÓN TÉCNICA ENTRE EL REGISTRO NACIONAL DE
LAS PERSONAS Y EL MINISTERIO DE JUSTICIA Y SEGURIDAD DEL GOBIERNO
DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES**

Entre la **DIRECCIÓN NACIONAL DEL REGISTRO NACIONAL DE LAS PERSONAS**, representada en este acto por su Director Nacional, Ingeniero JUAN JOSÉ BERNARDO D'AMICO, constituyendo domicilio legal en la calle Tte. Gral. J.D. Perón 664 de la Ciudad Autónoma de Buenos Aires, en adelante denominado "**RENAPER**", por una parte; y por la otra, el **MINISTERIO DE JUSTICIA Y SEGURIDAD DEL GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES**, representado en este acto por el Contador DIEGO SANTILLI, en función de las atribuciones encomendadas por el Decreto N° 391/18, constituyendo domicilio legal en la Avenida Regimiento Patricios N° 1142, de la Ciudad Autónoma de Buenos Aires, en adelante denominado el "**MINISTERIO**", en su conjunto denominadas como "**LAS PARTES**", acuerdan celebrar el presente Convenio de Cooperación Técnica conforme a los siguientes considerandos y cláusulas:

CONSIDERANDO:

Que la Ley N° 25.326 tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Que el Artículo 23, puntos 1, 2 y 3 de la mencionada norma dispusieron, respectivamente, que "Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales"; "El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad"; y que "los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

Que el Decreto N° 1.766/2011 (modificado por Decreto N° 243/17) creó el "Sistema Federal de Identificación Biométrica para la Seguridad" (SIBIOS), a fin de contribuir a la identificación de personas mediante información brindada a sistemas automatizados de identificación de huellas digitales y rostros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad;

Que de conformidad con el artículo 4 del Decreto mencionado, el Ministerio de Justicia y Seguridad del Gobierno de la Ciudad de Buenos Aires y el Ministerio de Seguridad

GOBIERNO DE LA CIUDAD DE BUENOS AIRES
ESCRIBANIA GENERAL
REGISTRADO BAJO EL N° 1555061
DL 2019
DGE GRAL
BUENOS AIRES, 01/03/2019

1

1

de la Nación suscribieron el "CONVENIO DE ADHESIÓN AL SISTEMA FEDERAL DE IDENTIFICACIÓN BIOMÉTRICA PARA LA SEGURIDAD PÚBLICA (DECRETO N° 1766/11)", registrado ante la Escribanía General de la Ciudad de Buenos Aires bajo el N° 10378 con fecha 12 de enero de 2012;

Por ello, y en razón de lo expuesto en los Considerandos precedentes, LAS PARTES convienen en suscribir el presente CONVENIO DE COOPERACIÓN TÉCNICA, conforme las siguientes cláusulas:

PRIMERA: El objeto del presente convenio es generar relaciones de cooperación y coordinación entre el **RENAPER** y el **MINISTERIO** dentro del ámbito de sus competencias.

SEGUNDA: El **RENAPER** facilitará, por la vía de excepción prevista en el artículo 23, inciso 2) de la Ley N° 25.326, el acceso a la información disponible en sus sistemas informáticos tendiente a identificar y/o verificar la identidad de las personas humanas sobre las cuales el **MINISTERIO** desarrolle las tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial nacional, provincial y de la Ciudad Autónoma de Buenos Aires, y durante la etapa de prevención e investigación de delitos de acción pública con arreglo a lo dispuesto en los artículos 184 del Código Procesal Penal de la Nación y 84 del Código Procesal Penal Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires.

Para dicha tarea, el **RENAPER** facilitará las fotografías del listado de personas que el **MINISTERIO** le requiera, indicando este último el nombre y Documento Nacional de Identidad que corresponda a cada una de ellas.

TERCERA: Los datos obtenidos por el **MINISTERIO** solo podrán ser utilizados por personal autorizado de su dependencia y al solo efecto de identificar y/o verificar la identidad del listado de personas que remita.

CUARTA: El acceso a la información proporcionada por el **RENAPER** se encontrará absolutamente restringido a cualquier miembro del personal del **MINISTERIO**, o terceros, que no se encuentren autorizados a tales fines. Asimismo, se encuentra prohibida la utilización de la información brindada por el **RENAPER**, para diferentes fines que los mencionados en la CLÁUSULA SEGUNDA del presente, como así también su cesión y/o transferencia a terceros, por vías gratuita u onerosa.

El **MINISTERIO** hará suscribir el ACTA DE CONFIDENCIALIDAD, que como Anexo forma parte integrante del presente, a todas las personas que autorice para hacer uso del referido servicio.

Los datos aportados por el **RENAPER** serán procesados por el "Sistema FACE-ID" que se implementará en el ámbito de la Ciudad Autónoma de Buenos Aires, mediante el cual, a través de una cámara fija, se reconocen los rostros de las personas registradas y cotejadas con registros provenientes de la Base de Datos del **RENAPER**, de acuerdo a la excepción prevista en el artículo 23, inciso 2) de la Ley N° 25.326.

QUINTA: El **MINISTERIO** dispondrá lo necesario para que la Policía de la Ciudad de Buenos Aires desarrolle un patrullaje específico en las sedes del **RENAPER** en el ámbito de la Ciudad Autónoma de Buenos Aires.

SEXTA: LAS PARTES convienen que toda situación no prevista que implique una modificación del presente convenio, será objeto de una Adenda a suscribir entre el **RENAPER** y el **MINISTERIO**.



SÉPTIMA: En conformidad con los términos del artículo 23, inciso 3) de la Ley N° 25.326, el **MINISTERIO** cancelará la información que el **RENAPER** le hubiera remitido, una vez que los datos hayan dejado de ser necesarios para la finalidad requerida, procediéndose a su destrucción.

Al momento de procederse a la cancelación de la información se labrará un Acta en presencia de un representante del **RENAPER**, a fin de acreditar la destrucción de la información indicada precedentemente.

OCTAVA: El presente convenio tendrá vigencia desde su suscripción y posterior aprobación mediante Disposición del DIRECTOR NACIONAL del **RENAPER**, por el plazo de UN (1) año, prorrogándose automáticamente por el mismo término, salvo que alguna de **LAS PARTES** lo denuncie, con una anticipación no menor a TREINTA (30) días, sin generar este último temperamento, derechos a reclamos de naturaleza alguna.


NOVENA: A todos los efectos legales, **LAS PARTES** constituyen domicilios en los indicados en el encabezamiento, donde serán válidas todas las notificaciones, prorrogando la jurisdicción y competencia en los Tribunales en lo Contencioso Administrativo Federal de la Capital Federal, con exclusión de cualquier otro fuero que pudiese corresponder.

Se deja expresa constancia que sólo se tendrán por válidas todas aquellas notificaciones judiciales o extrajudiciales que se hicieran al MINISTERIO en el domicilio del Departamento de Oficios Judiciales y Cédulas de la Procuración General ubicado en la calle Uruguay 458 de esta Ciudad, conforme a lo dispuesto por el artículo 20 de la Ley N° 1.218 y la Resolución N° 77/PG/06.

En prueba de conformidad, se suscriben tres (3) ejemplares de un mismo tenor y a un sólo efecto, en la Ciudad Autónoma de Buenos Aires, a los 26 días del mes de febrero del año dos mil diecinueve.



Ing. JUAN JOSE D'AMICO
Director Nacional
Registro Nacional de las Personas



Diego César Santilli
p/p Decreto N° 391/18
Ministerio de Justicia y Seguridad

ANEXO

ACTA DE CONFIDENCIALIDAD

En la Ciudad Autónoma de Buenos Aires, a los.....días del mes de.....del año....., el/la Sr/Sra....., titular del DNI:....., en su carácter de personal dependiente autorizado por el Ministerio de Justicia y Seguridad del Gobierno de la Ciudad de Buenos Aires, procede a suscribir la presente Acta de Confidencialidad, en cumplimiento de lo dispuesto en la CLÁUSULA CUARTA del Convenio de fecha....., celebrado entre el **REGISTRO NACIONAL DE LAS PERSONAS** y el **MINISTERIO DE JUSTICIA Y SEGURIDAD DEL GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES**. En tal sentido, declara bajo juramento, guardar absoluta reserva y asume el compromiso de no divulgar los datos, métodos, procedimientos y todos otros hechos o actos u omisiones de los que tome conocimiento en ocasión del cumplimiento del Convenio antes referido, bajo apercibimiento de las penalidades previstas en el Código Penal y en las disposiciones vigentes en materia de secreto o reserva administrativa.



Ing. JUAN JOSE D'AMICO
Director Nacional
Registro Nacional de las Personas



GOBIERNO DE LA CIUDAD DE BUENOS AIRES

Hoja Adicional de Firmas
Anexo

Número:

Buenos Aires,

Referencia: 7555081-2019

El documento fue importado por el sistema GEDO con un total de 6 pagina/s.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.03.07 15:23:29 -03'00'

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.03.07 15:23:30 -03'00'

ANEXO

IV



G O B I E R N O D E L A C I U D A D D E B U E N O S A I R E S

"2019 -Año del 25º Aniversario del reconocimiento de la autonomía de la Ciudad de Buenos Aires"

Número: NO-2019-37063734-GCABA-DGEYTI

Buenos Aires, Jueves 28 de Noviembre de 2019

Referencia: s/ Traslado - "O.D.I.A. c/ G.C.B.A. s/ Amparo", Expte. N° 9480/19

En respuesta a: NO-2019-36752604-GCABA-DGALSE

A: Fabiana Costanza (DGALSE),

Con Copia A:

De mi mayor consideración:

Tengo el agrado de dirigirme a Ud., atento a lo solicitado por la Procuración General de la Ciudad de Buenos Aires, mediante NO-2019-36216913-GCABA-DGAIP, en relación a los autos caratulados "O.D.I.A. c/ G.C.B.A. s/ Amparo", Expte. N° 9480/19, en trámite por ante el Juzgado de Primera Instancia en lo Contencioso, Administrativo y Tributario N° 23, Secretaría N° 45.

Para comunicarle que:

Pregunta N.10

La información desde que es capturada hasta que llega al CMU, viaja encriptado mediante aplicabilidad del protocolo 3DES.

Pregunta N.13

Como ya hemos respondido oportunamente, el SRFP no almacena imágenes de las lecturas realizadas, excepto sea una lectura positiva. Es decir, que la persona se encuentra en la base de datos del CONARC impartida por la justicia. En estos casos, estas imágenes reciben el mismo tratamiento que el estipulado en la Ley original N. 2602/08 abrogada por la ley 5688/16.

Pregunta N.39

Una vez utilizados los medios tecnológicos ya mencionados (Morpho Touch) y no habiendo éxito en la identificación de la persona, se realiza el procedimiento policial ordinario para aquellos casos de validación de datos filiatorios.

Pregunta N.44

Como se mencionara precedentemente, los dispositivos utilizados utilizan un Smartphone con tecnología

LIONEL A. CASTELLINO
Secretario

4G; sistema operativo Android de la marca Samsung -en sus diferentes modelos-, están interconectados a la red del MJYS a través de un APN provista por la firma Telefónica de Argentina S.A. Estos equipos tienen instalado el sistema MDM y Airwatch, lo que hace que el mismo sea un quiosco y no tenga ningún tipo de conexión hacia otras redes de datos que no sea lo provisto por este Ministerio. Una vez tratadas las alertas positivas, estas se eliminan del equipo de forma automática.

Pregunta N.45

Como ya se mencionara, los teléfonos institucionales provistos reciben las alertas a través de una ampliación donde enuncia; la foto de la persona prófuga de la justicia, número de cámara de video que la detectó y toda aquella información de la causa judicial extraída del CONARC.

La accesibilidad a esta aplicación únicamente es obtenida por personal policial asignado a estos operativos dentro de la red del MJYS.

Pregunta 61

Dependiendo de la calidad de las imágenes obtenidas del cruzamiento de la base de datos de CONARC con el RENAPER, se utiliza alguno de los métodos siguientes: holístico, locales, o Geométricos,

Como set de datos para calibrar y verificar el funcionamiento del sistema, se realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los caso los porcentajes de error exigidos.

DGEYTI - Pregunta 62

Como set de datos para calibrar y verificar el funcionamiento del sistema, se realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los casos los porcentajes de error exigidos.

DGEYTI - Pregunta 67

Conforme a la resolución 398/2019 en su artículo 3, se invita a la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires a auditar el funcionamiento del SRFP, a cuyo fin se concluyeron reuniones informativas y demostrativas de procedimientos reales en el Centro de Monitoreo Urbano – Centro Operativo del SRFP.

Asimismo, se remitió la información técnica requerida a la Defensoría del Pueblo conforme al funcionamiento técnico y operativo del SRFP.

Pregunta 76 y 77

El pliego de bases y condiciones mencionado, incluía dos sistemas, es SRFP y un sistema de análisis forense de imágenes y predictivo. Todas las preguntas solicitadas en estos puntos, corresponden a los sistemas mencionados en segunda instancia, los cuales no son objeto del presente requerimiento.

Sin otro particular saluda atte.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.11.28 17:06:19 -03'00'

PORNO CARLOS TRISTAN
Director General
D.G. DE ESTUDIOS Y TECNOLOGIAS DE LA INFORMACION
MINISTERIO DE JUSTICIA Y SEGURIDAD


MONICA CASTELLÓN
ABOGADO
Tº 27 - Dº 14.5.61

Digitally signed by Comunicaciones
Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.11.28 17:06:20 -03'00'

ANEXO V

SUCESOS / RECONOCIMIENTO FACIAL

Cayeron 7 prófugos detectados con el nuevo sistema de reconocimiento facial



RASTREO. De prófugos. (Policía de Ciudad de Buenos Aires/Télam)

Fueron capturados a pocas horas de la puesta en marcha del sistema de reconocimiento facial. El software realiza el reconocimiento en diversas condiciones de iluminación y ángulo. También, ante cambios de apariencia como ser anteojos, bigotes, gorras y peinados.



Viernes, 26 de abril de 2019 - 08:01 hs

Siete delincuentes que se encontraban prófugos de la Justicia fueron detenidos hoy a pocas horas de la [puesta en marcha del Sistema de Reconocimiento Facial](#) que fue incorporado a las cámaras de seguridad de la ciudad de Buenos Aires, anunció el jefe de Gobierno porteño, Horacio Rodríguez Larreta.

Durante la presentación oficial del sistema, Rodríguez Larreta sostuvo que “este es un paso más que estamos dando en incorporar tecnología para cuidar a la gente” y agregó que “nuestro único objetivo en esto es que los vecinos de la ciudad estén más seguros y no estén en la calle caminando alrededor de delincuentes”.

“Ya venimos probando este sistema y la verdad que funciona muy bien: en el día de hoy solamente, en lo poco que va de esta mañana, ya se identificaron 11 casos, de los cuales siete pudieron ser detenidos e identificados y puestos a disposición de la Justicia”, explicó el jefe de Gobierno.

Remarcó que el software que se está utilizando en las cámaras “es la tecnología de punta que se está usando en el mundo, es lo mejor que hay” y felicitó a todo el equipo del Ministerio de Seguridad porteño por este avance.

NEWSLETTER: LOS TÍTULOS DEL DÍA

Los titulares de nuestra edición, a primera hora de la mañana.

Ingresá tu E-mail

Rodríguez Larreta estuvo acompañado por el vicesjefe a cargo del Ministerio de Justicia y Seguridad, Diego Santilli; el subjefe de la Policía de la Ciudad, Gabriel Berard, y por la ministra de Seguridad de la Nación, Patricia Bullrich, entre otros funcionarios.

Desde esta mañana, 300 cámaras de la ciudad de Buenos Aires comenzaron a buscar a 40.000 fugitivos, de los cuales el 67 por ciento se cree que están ocultos en la zona metropolitana, a partir de la puesta en marcha del Sistema de Reconocimiento Facial de Prófugos, un software ruso que se utilizará por primera vez en el país.

Santilli detalló que los datos de los prófugos surgen del sistema de Consulta Nacional de Rebeldías y Capturas (Conarc) del Registro Nacional de Reincidencia, los cuales son públicos y se pueden consultar por [internet](#).

“Estamos hablando de ir a buscar y detener a los más de 40.000 prófugos que tiene el sistema judicial argentino, entre los que hay 1.300 personas buscadas por homicidios, 1.500 por delitos sexuales, 15.000 por robos y hurtos y 2.300 por narcotráfico”, detalló ayer el funcionario en un encuentro con la prensa gráfica.

El software, llamado Danaide, fue instalado en 300 cámaras rotativas de un total de 7.000 que tiene la Ciudad y en la práctica, cuando detecte el rostro de algún prófugo, emitirá un alerta y se enviará al lugar al personal de calle que se encuentre más cerca para detenerlo, salvo que se trate de algún delincuente muy peligroso y sea necesario recurrir a un equipo especial, indicó la comisario Raquel Cesanelli, jefa del Centro de Monitoreo Urbano.

Agregó que una vez que se encuentre a la persona buscada, se le solicitarán sus datos filiatorios y en caso de confirmarse, se consultará al juez si todavía requiere a ese fugitivo y las medidas por adoptar; la confirmación final de quién se trata se hará a través de las huellas digitales.

Por su parte, Cecilia Amigo, jefa de gabinete de la Secretaría de Administración, explicó que “el sistema tuvo una efectividad del 92 por ciento en las pruebas piloto, que actualmente se utiliza en China y Rusia y es considerado uno de los mejores del mundo”.

La tecnología adquirida, que tuvo un costo de 2,3 millones de pesos para el Gobierno porteño, puede buscar en la base de datos en menos de medio segundo y realiza el reconocimiento facial en diversas condiciones de iluminación y ángulo de

escena, aun ante cambios de apariencia como ser anteojos, barba, bigotes, gorras o sombreros y peinados.

Tenemos algo para ofrecerte

Con tu suscripción navegás sin límites, accedés a contenidos exclusivos y mucho más. ¡También podés sumar **La Voz** para ahorrar en cientos de comercios!

[VER PROMOS DE SUSCRIPCIÓN](#)

TEMAS RELACIONADOS

RECONOCIMIENTO FACIAL

BUENOS AIRES

MÁS DE SUCESOS

SUCESOS

Radiografía de los secuestros extorsivos en Argentina: la cantidad de 2021 y el tiempo de cautiverio

SUCESOS

Más de 120 mil evacuados por inundaciones en China

SUCESOS

Un adolescente quedó en medio de una pelea barrial y recibió un disparo en la cabeza


SUCESOS

Continuarán presos los acusados de estafar con la venta de terrenos en Punilla

11 de octubre de 2021 Edición Impresa 

Defendé la otra mirada por \$300 x mes




 Iniciar sesión

Hacete soci@ →

 Ingresar

Hacete soci@ →

11 de octubre de 2021

Edición Impresa 

Hoy:

Líbero

Secciones y Suplementos



Hoy:

Líbero

Secciones

[El país](#) [Economía](#) [Sociedad](#) [Espectáculos](#) [Deportes](#) [Ciencia](#) [El mundo](#) [Edición impresa](#) [Universidad](#) [Ajedrez](#) [Cultura](#) [Diálogos](#) [Plástica](#) [Psicología](#) [Cartas de lectores](#) [Contratapa](#) [Audiovisuales](#) [Recordatorios](#) [Consumo](#) [Salta](#) [Catamarca](#) [12Podcasts](#) [Soci@s](#) [La ventana](#)

Suplementos

[Cash](#) [Enganche](#) [Radar](#) [Turismo](#) [Radar Libros](#) [NO Soy](#) [Las 12](#) [Universidad](#) [Sátira](#) [12M2](#) [Rosario](#) [12Verano](#) [12Líbero](#) [Especiales de P12](#)



[El país](#)

[Economía](#)

[Sociedad](#)

[Cultura y Espectáculos](#)

[Deportes](#)

[El mundo](#)

[Cultura](#)

Hoy:

Líbero

Buscar... 



Sociedad

Una mujer erróneamente detectada por el sistema de Reconocimiento Facial

Detenida por el parecido con una persona buscada

El cuestionado método implementado en la ciudad para encontrar personas prófugas de la Justicia comenzó a mostrar sus riesgos: una joven estuvo un día detenida porque el sistema detectó un 83 por ciento de parecido a la verdadera sospechosa. También hubo varios casos de trabajadores del subte "reconocidos" falsamente.



La detención se produjo en el subte, donde están algunas de las 300 cámaras rotativas.. Imagen: NA

A veinte días de estrenado el sistema de Reconocimiento Facial de Prófugos, y pese a que durante su lanzamiento las autoridades aseguraron que nadie iba a quedar detenido por equivocación o sin debida justificación, algunos ciudadanos comenzaron a sufrir los errores o excesos del gran hermano porteño. Una mujer fue detenida y liberada un día después porque no era la persona buscada: sólo se parecía a una prófuga; además, varios trabajadores del subterráneo fueron demorados y debieron ser resguardados por sus compañeros tras haber sido identificados como sospechosos por el sistema. Al estrés y la humillación que significa ser detenido en la vía pública, se suma el papeleo y la pérdida de un día de trabajo. El integrante del Grupo de Litigio Estratégico Adrián Albor, que podría representar a la mujer detenida, si finalmente decide iniciar acciones legales, dijo que “un funcionario público que acepta un sistema con falencias tiene dolo eventual de la privación ilegal de la libertad”.

La detención se produjo en el subte porteño donde están activas algunas de las 300 cámaras rotativas, de las 7000 que tiene el Sistema Integral de Video Vigilancia de la Ciudad, para rastrear a las personas buscadas por el Sistema de Consulta Nacional de Rebeldías y Capturas (Conarc). Una base pública dependiente del Ministerio de Justicia y Derechos Humanos de la Nación.

La mujer detenida por su parecido fue esposada y trasladada a la comisaría el martes a la noche, luego de que se disparara un alerta del sistema de Reconocimiento Facial. Según contó una amiga, la policía le informó que tenía una causa por fraude habitacional en 2011, pese a que la mujer negó el hecho y mostró su DNI para acreditar su identidad.

Tras varias horas por averiguación de antecedentes y después de que le aseguraran a la amiga que tenía orden de liberación, la trasladaron a otra comisaría en la calle Suipacha, donde permaneció incomunicada, porque no tenía ni abogado, ni familiares en la ciudad, los únicos autorizados a verla. El miércoles fue liberada después de que se constatará que no tenía ninguna causa judicial: no era ella la persona buscada por la justicia.

“El avasallamiento de libertades que hace el Estado es muy grande cuando autoriza un sistema que tiene un importante margen de error y que le puede arruinar la vida a una persona metiendo gente presa por las dudas”, dijo Albor.

“Se está vulnerando el derecho a la intimidad. No puede ser que una persona camine con miedo de que una cámara lo confunda con alguien que está siendo buscado por la justicia. Se coarta la libertad de caminar libremente sin sentir que vivimos en 1984 de (George) Orwell”, dijo el letrado, quien remarcó que “el Código Procesal permite llevar preso a una persona con pedido de captura, pero no a una porque se le parece, por las dudas”.

Según informaron desde el Ministerio de Seguridad porteño, “la policía y el ministerio lo que hacen es poner a disposición de la justicia a las personas con pedidos de captura que aparecen en la base de datos, donde figura el nombre y la causa (182 personas desde que comenzó a funcionar)”.

“Hay un protocolo de actuación cuando se da el alerta, y una vez que se identifica a la persona se llama al juzgado interviniente”, dijeron, y le pasaron la pelota al Poder Judicial porque, aseguraron, “es la justicia la que decide si libera, detiene o demora”.

En ese pase de factura, son los ciudadanos los que quedan atrapados, como le pasó a una empleada doméstica detenida la semana pasada, también en el subte, tras ser identificada por el sistema de reconocimiento como una persona buscada por el, a veces, excesivo celo judicial.

La mujer fue sacada de un vagón mientras la gente le gritaba “chorra” y detenida por la policía a las 10 de la mañana en Constitución, por una causa del año 2006, según el alerta del sistema. Fue trasladada a la Alcaldía 1 e incomunicada, mientras una de sus empleadoras, que contó la situación en las redes sociales, intentaba aclarar la situación. Finalmente, fue liberada a las once de la noche. Y menos de una semana después, su causa quedó extinguida y se le dictó el sobreseimiento.

Si llegaste hasta acá...

Es porque te interesa la información rigurosa, porque valorás tener otra mirada más allá del bombardeo cotidiano de la gran mayoría de los medios. Página/12 tiene un compromiso de más de 30 años con ella y cuenta con vos para renovarlo cada día. Defendé la otra mirada.

Defendé tu voz.

Únete a Página/12

INGRESAR

Hacete soci@ para contribuir

Un sistema polémico

Identificaron a 14 personas por día con el reconocimiento facial, pero el 81% quedó libre

Hay cámaras en las estaciones de subtes y trenes. Reconocieron a 1.227 personas en 88 días y sólo 226 quedaron detenidas. El resto eran errores en la base de datos.



La detención de un hombre acusado de abusar de menores, a través del Sistema de Reconocimiento Facial, en el subte A.

Natalia Iocco

0

22/07/2019 17:49 | Clarín.com **Policiales** | Actualizado al 22/07/2019 21:17



Es lunes y
está punto

salen en un corral. Dos cosas de civil. La única anormalidad es una mujer: rodean a un joven que pone cara un poco de ofuscado, porque está a punto de perder el tren, y otro poco de susto porque no sabe bien qué está pasando.

Esta escena se repite: el nuevo sistema de reconocimiento facial en las estaciones de subtes y, ahora, en las de ferrocarriles, de la ciudad de Buenos Aires, activó 1.227 alertas. Según datos oficiales, desde la implementación del Sistema de Reconocimiento Facial de Prófugos (el 25 de abril), se identificaron a 14 personas por día, en promedio.

De esa cifra, sólo el 18 por ciento quedó detenido. **El resto fueron notificadas, no tenían requerimientos judiciales que implicaran una detención o padecieron un error del sistema o de la base de datos.**



Se trató de 1001 casos en los que transeúntes fueron demorados por la Policía en las estaciones hasta constatar su situación con el juzgado interviniente. De ese universo, casi la mitad correspondieron a datos mal cargados en la base de datos.

“Del total, 10 estaban acusados de homicidio, 13 por delitos sexuales, 11 por causas vinculadas a drogas y 57 por robos y hurtos”, informaron en el Ministerio de Seguridad y Justicia de CABA.

Pero ¿qué pasa con el 82% restante?

Leandro Colombo Viñas (37) había ido al banco el 26 de junio y regresaba a la oficina a eso de las 15. Había leído un poco. Conocía el anuncio y sabía de la tecnología que aplican para identificar personas porque tiene una empresa de sistemas: los softwares son lo suyo.

Mirá también

Detienen en el subte a un abusador de menores con el sistema de reconocimiento facial

Lo detuvo, primero, un policía que le pidió el documento y empezó a cargar datos en uno de sus tres teléfonos celulares. “Me llamó la atención. Pensé que había dado un falso positivo y esperé tranquilo para irme lo más rápido posible, nunca se me pasó por la cabeza que hubiera una causa en mi contra. No recuerdo cuánto tiempo después llegó un segundo policía. Les preguntaba cosas, charlamos un poco mientras tanto”, le contó a Leandro a **Clarín**.

"Le doy el documento y no le coincide el nombre ni el apellido con el número de DNI. Habla con la jefa de servicio, me pregunta si tengo otra documentación y le doy el registro. Hasta la credencial del club le entregué. Ahí me dicen que con mi número de DNI había una causa por robo agravado por uso de arma de fuego. Me llamó la atención porque era imposible, me empecé a preocupar un poco más cuando vi que tenía mi foto, la de mi documento. Siguió hablando hasta que su jefa le avisó que tenía que llamar al juzgado para que definan qué querían hacer conmigo y ahí pensé *‘listo, con los tiempos de la Justicia no me voy más’*”, agregó. (x)



Leandro Colombo Viñas fue demorado en una estación de subte mediante el sistema de reconocimiento facial. Foto: Fernando de la Orden.

Pasaron tres llamados al juzgado y más de tres horas. La rutina del día, perdida: “Pasada una hora y después de tres llamados al juzgado, fuimos a la comisaría, me tomaron las huellas y me sacaron fotos. Habré estado una hora más acreditando que yo era yo. Tres personas trabajando, tomándome los datos, una pérdida de recursos total. Quizá si toda esa gente hubiera estado en la estación se evitaban más robos, no sé. Después otra hora llenando actas para que quedara un registro y tuvimos que volver a buscar testigos. Se me hicieron las 18.30”, recordó el joven a quien no le entregaron ninguna constancia de esos trámites.

Para el ministerio de Seguridad de la Ciudad, el margen de error es mínimo. “Sólo el 4 % de los casos pueden tener un falso positivo, que quiere decir que el sistema se equivoca o confunde el rostro de una persona con el de otra”, aclaran. El software que entrecruza los registros de 46 mil prófugos con las imágenes de 300 cámaras que se van alternando en estaciones de subte y lugares transitados, tenía un margen de error cercano al 7%, según las previsiones de los técnicos, ahora dicen que se reduce cada vez más.

"Es algo parecido a pescar con red en el mar. Tenemos casos de personas demoradas 8 ó 10 horas por errores de ese tipo. Desde los datos mal cargados hasta causas por no presentarse como testigo en un juicio. Pero no hay otra manera que enviar oficios para aclarar,


de Carmen Vela, de Conarc.

En los últimos días, la ministra de seguridad de la Nación, Patricia Bullrich, anunció que se implementará en las estaciones de ferrocarril. Ya funciona en Retiro, en dos semanas también se implementará en Constitución y Once y, en septiembre, en Chacarita. Estiman que por estos puntos se mueven 750 mil personas.

El alerta llega a la Policía porteña que derivará la información a la Federal, con jurisdicción en las estaciones.

Mientras en el mundo se debate la seguridad de datos y los riesgos de la identificación compulsiva de este sistema, en Buenos Aires **la tecnología se topa con la burocracia.**

La base de datos usada para nutrir el software de reconocimiento facial es de la [Consulta Nacional de Rebeldías y Capturas \(Conarc\)](#). Allí son de acceso público todos los pedidos de captura de personas con requerimiento de la Justicia.

Pero, como le pasó a María Raquel Holway (54), fundadora de Alerta Vida, una ONG que -entre otras iniciativas- impulsa investigaciones contra la pedofilia y la trata de personas, la información está desactualizada. 

una terminal de Retiro y decidieron tomar el subte para llegar más rápido. Eran las ocho de la mañana y dos policías la "corrieron" adentro de un vagón.



María Raquel Holway (54), fundadora de Alerta Vida, fue demorada por el sistema de reconocimiento facial. Foto: Fernando de la Orden.

"Puse un pie en el vagón y me corrieron adentro del subte como si fuera Pablo Escobar. Los miré y dije: ¿Me están corriendo a mí? 'Listo, me armaron una causa', pensé", le contó la mujer a **Clarín**.

"Acababa de cruzarme todo el país, he presentado el DNI. Salí del país y no tuve ningún problema. En ese momento me avisan que tengo una captura internacional. Cuando me dicen el año, era de 2002, me di cuenta. Es una causa que me generó una denuncia de mi ex, un violento condenado, en la que me acusó de salir del país con mi hijo, cuando me escapaba de él. Me sobreseyeron cuando regresé a Argentina en 2004. Fueron presentados los oficios, ya estaba todo resuelto hace años", explicó Raquel.

Lo cierto es que la retuvieron alrededor de una hora hasta que el juzgado resolviera su situación. "Tuve que mandar otro oficio para que me saquen porque ahí mismo llamaron y les dijeron que yo no tenía ningún requerimiento por esa ni por otras causas. Mientras y ⊗ estaba ahí había otros dos en la misma situación. Había ocho policías rodeándonos", recordó.



sensorial" en Ezeiza para detectar a traficantes

El director del Registro Nacional de Reincidencia del Ministerio de Justicia de la Nación, José Guerrero, explicó a **Clarín** que estos casos corresponden a la **falta de actualización del Poder Judicial sobre los requerimientos**. Aunque dijo "que se depura la base de datos a medida que surgen estas notificaciones", confirmó que deben presentarse oficios judiciales para eliminar los datos de las personas inocentes de esa base de datos y que en pocos minutos pueden ser removidos.

Newsletters Clarín Qué pasó hoy

Te contamos las noticias más importantes del día, y qué pasará mañana cuando te levantes



Recibir newsletter



TEMAS QUE APARECEN EN ESTA NOTA

Reconocimiento Facial



Comentarios

INFOBAE

Reconocimiento facial en la ciudad de Buenos Aires: cómo será el sistema que ayudará a capturar a los 46 mil prófugos de la Justicia

Se pondrá en marcha mañana a primera hora. Habrá 300 cámaras rotativas destinadas a encontrar a aquellos delincuentes que tienen pedido de captura



Por **Mauricio Luna**

24 de Abril de 2019

mluna@infobae.com



El reconocimiento facial permitirá detectar al instante si esa persona está prófuga de la Justicia

A partir de la primera hora del jueves, en la ciudad de Buenos Aires comenzará a funcionar el **Sistema de Reconocimiento Facial de Prófugos (SRFP)**. Se trata de un mecanismo que operará directamente con otro sistema, el de **Consulta Nacional de Rebeldías y Capturas**

El sistema de monitoreo por cámaras de video vigilancia que tiene en marcha la policía

en la Argentina: **1.300 por homicidio, 1.500 por delitos sexuales, 15.000 robos y hurtos, 2.300 por narcotráfico...** Delincuentes buscados por la Justicia, la cual le pide a todas las fuerzas de seguridad que se los traiga a disposición".

El SRFP está destinado a la **detección, verificación, identificación y detención de personas sobre las cuales exista una orden de captura.** El CONARC actualizará el listado todos los días a las 7 de la mañana, lo que le permitirá al SRFP actualizarse automáticamente.



Los efectivos mirarán las imágenes y aparecerá un alerta cuando se reconozca una cara

Para su desarrollo se utilizarán 300 de las más de 7.000 cámaras de monitoreo que posee la ciudad. A través de un software ruso, cada cámara tendrá una licencia. Las mismas **serán rotadas durante las 24 horas** considerando los diversos puntos en donde haya más tránsito de personas.

"El objetivo es que estos delincuentes no convivan con nosotros todos los días. La primera garantía es la de la privacidad: **el sistema sólo trabaja con los prófugos aportados por el CONARC,** una base pública que puede leer cualquier ciudadano del país", explicó Santilli.



El sistema fue presentado por Diego Santilli junto a Raquel Casanelli (comisario de la Policía de la Ciudad), Cecilia Amigo, jefa de gabinete de la secretaría de Administración de Seguridad y Aníbal Falivene, subsecretario de Investigaciones y Estadística Criminal

El software costó \$2.300.000 y tendrá validez por 17 meses. En el monto se contemplaron los servidores de procesamiento, el desarrollo, las licencias mencionadas y la instalación de nuevas cámaras de seguridad.

"Detecta rostros de perfil, con gorra, capucha y semicubiertos. En todas las pruebas que hicimos fuimos cambiando la fisonomía (la barba, por ejemplo) de la persona. Todo cambio fuera de los rasgos faciales los detecta absolutamente. Si la persona lleva un casco de moto puesto no. **Las pruebas fueron 100% eficientes**", sostuvo Amigo.

"Podemos ampliar las licencias al 100% cuando lo decidamos o necesitemos. Desde la arena operativa sería imposible cumplir con la demanda que se requeriría para completar el tc las cámaras", aclaró la jefa de gabinete.



Cuando salte el alerta, mostrará rápidamente el rostro y determinará cuál fue la cámara que la detectó

Aníbal Falivene, subsecretario de Investigaciones y Estadística Criminal, manifestó que las fotografías son **"entregadas por un convenio que firmamos con el Registro Nacional de las Personas (RENAPER)**. El extranjero que no haya tramitado el DNI no va a estar. Sí va a estar en otro tipo de bases, como por ejemplo las fotografías que aporte Migraciones".

Cuando el sistema detecte una coincidencia, el Centro de Monitoreo Urbano procederá a **generar una carta de servicio y dará aviso al personal policial más cercano para que intervenga**, actuando de conformidad con los protocolos que rigen la Línea de Atención de Emergencia del 911.

"Tenemos desarrollada **una app específica, que alerta estos positivos que llegan a los teléfonos institucionales de los efectivos lindantes** a la cámara que emite el alerta. Además de incluir el nombre, el apellido, la tipología de causa y las imágenes de la persona buscada, también **se compartirá un mapa específico que indicará cuál es la cámara que emitió ese alerta**", dijo Amigo.



[Últimas Noticias](#)[Política](#)[Sociedad](#)[Deportes](#)[Tecno](#)[Economía](#)

Santilli se mostró muy entusiasmado con este nuevo programa

En cuanto a los datos biométricos de las personas no buscadas, **los funcionarios explicaron que no serán guardados en la base de datos**. De quienes sí lo sean, el sistema archivará el resultado durante 60 días.

"Son delitos muy graves, no es cualquier cosa. Si sirve estamos a disposición para ayudar.

Podemos poner este sistema porque venimos haciendo la arquitectura a través de cámaras 4K y HD desde hace dos años. No digo que las anteriores hayan sido malas, sino que era lo que había en su momento", concluyó Santilli.

Seguí leyendo:

[El gobierno porteño comenzó la construcción de gradas panorámicas a metros del Obelisco](#)

[Cuál es el perfil de campaña con el que quieren presentar a Larreta](#)

TEMAS RELACIONADOS

[Ciudad de Buenos Aires](#)[Diego Santilli](#)[reconocimiento facial](#)

ÚLTIMAS NOTICIAS

Cáncer: un nuevo tratamiento destruyó tumores en enfermos terminales y aumentó la sobrevida

Científicos del Instituto de Investigación del Cáncer de Londres probaron una combinación de fármacos de inmunoterapia que resultó eficaz y tuvo menos efectos secundarios que la quimioterapia . Aquí detalles del estudio



Balazos en la madrugada y persecuciones policiales: la barra de Los Andes aterroriza Lomas de Zamora

Mañana juega el Milrayitas y el miedo recorre el barrio. Una guerra de guerrillas se instaló en el medio de la interna por ocupar el liderazgo en las tribunas



La dramática revelación de Fran Mariano, ex Cuestión de Peso: “Tengo cicatrices en el cuerpo porque mi papá me pegaba por ser gay”

Franco brindó una entrevista televisiva donde brindó detalles sobre su obesidad, su adicción a las cirugías y la violencia ejercida por su padre por su elección sexual

Detuvieron al segundo máximo comandante del ISIS: Estados Unidos ofrecía 5 millones de dólares por su captura

Sami Jasim manejaba las finanzas del sangriento califato y llegó a ser el número dos de Abu Bakr al-Baghdadi. Fue arrestado en Turquía por los servicios secretos de Irak



NOTAS de ACTUALIDAD

[INICIO](#) [ECONOMÍA](#) [POLÍTICA](#) [SOCIEDAD](#) [DEPORTES](#) [MUNDO](#) [PASTILLERO](#) [ZOOM DE PERIODISTAS](#) [SHOW](#)

Santilli destacó la efectividad del Sistema de Reconocimiento Facial

27 abril, 2019 NdA



El vicejefe de gobierno porteño indicó que “hay más de cuarenta mil personas en situación de pedido de captura y que la justicia pide que se presenten”. En las primeras 48 horas del mecanismo cayeron varios prófugos.



El jueves pasado por la mañana comenzó a utilizarse el nuevo Sistema de Reconocimiento Facial que presentó el gobierno de la ciudad de Buenos Aires. Durante el primer día, siete prófugos de la Justicia lograron ser identificados y detenidos, mientras que en las últimas horas se sumó el caso más emblemático: un hombre de 50 años acusado por violación que era buscado desde 2017.

En ese marco, el vicejefe de Gobierno porteño Diego Santilli aportó más detalles de este mecanismo, al cual calificó como “100% efectivo hasta el momento”. “Con el plantel de 7 mil cámaras, es diferente al lector de patentes porque esto sólo opera con la base de


Seguinos en Facebook



datos de personas prófugas. Es una base de datos pública del Ministerio de Justicia de la Nación, donde todas las provincias van integrando allí todas las personas buscadas”, señaló el funcionario en diálogo con Sábado Tempranísimo por Radio Mitre.

Con respecto al funcionamiento, el segundo de Horacio Rodríguez Larreta explicó que “la cámara detecta a la persona y le envía un aviso automático a la policía que está en la zona donde está activada esa cámara. El agente acude al lugar, verifica la identidad del sospechoso buscado y de ser la persona se da aviso a la justicia y se lo pone a disposición”.

Santilli resaltó que actualmente “hay más de cuarenta mil personas en situación de pedido de captura y que la justicia pide que se presenten”. “No le podemos pedir a la policía que conozca 46 mil caras, es imposible recordarlas y por eso pusimos un sistema para poder trabajar más tranquilos”, concluyó.


Política, Último Momento  diego santilli, Sistema de Reconocimiento Facial

« Pignanelli: “Las medidas anunciadas son en contra de la sustentabilidad”

Moyano: “La que va a parar es la gente, esto va más allá de los dirigentes” »

Entradas relacionadas



10 octubre, 2021  NdA


0

Menéndez reconoció que el Frente de Todos «no ha podido estar a la altura de las expectativas de la gente»

El candidato a diputado nacional por el oficialismo afirmó que «la pandemia nos pegó después de...

Noticias Destacadas Política



10 octubre, 2021  NdA


0

El frente de Hotton comienza a sumar apoyos tras superar el piso en las PASO

La candidata a diputada nacional por +Valores afirmó que el oficialismo y la oposición «están preocupados...

Noticias Destacadas Política



10 octubre, 2021  NdA

0

CFK defendió a Axel Kicillof ante las críticas por sus anuncios para egresados

La vicepresidenta señaló que el diario Clarín «no dijo nada» cuando el expresidente Mauricio «Macri le...

Noticias Destacadas Política

DEJA TU COMENTARIO

Comenta

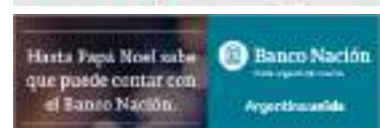
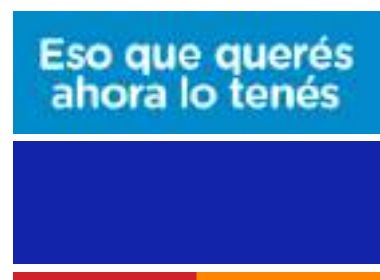
Nombre

Correo electrónico

URL de la web

CONVIVIR ES CUIDARNOS.

LEGISLATURA
GOBIERNO DE BUENOS AIRES



INFOBAE

Un hombre estuvo seis días preso por un error policial

Guillermo Ibarrola fue detenido en la terminal de Retiro. Lo confundieron con un hombre buscado por un robo agravado cometido en Bahía Blanca hace tres años

2 de Agosto de 2019

Play

La vida de **Guillermo Federico Ibarrola** se transformó en un infierno de seis días por un error policial. Ibarrola, de 39 años, fue detenido el sábado pasado en el barrio porteño de **Retiro acusado de haber cometido un robo agravado en 2016 en Bahía Blanca**. De acuerdo a la base de datos del sistema que utiliza la Policía de la Ciudad tenía un pedido de captura del Juzgado de Garantías N° 2 de esa ciudad bonaerense.

Pero cuando Ibarrola era trasladado a una cárcel provincial los investigadores del caso advirtieron que había habido un error. "Cuando lo buscaron, había 23 con ese nombre en todo el

bien, pero estaba mal cargada la búsqueda", argumentaron fuentes judiciales a la agencia estatal *Télam*.

"Nunca pensé que me iba a tocar vivir algo así. Me tocó a mí pero le puede tocar a cualquiera", comentó la víctima en la terminal de Retiro, lugar al que llegó en micro después de haber sido traslado al juzgado de **Bahía Blanca**, donde había sido detenido casi una semana antes.



Guillermo Federico Ibarrola tiene 39 años

Cuando los agentes lo aprehendieron el sábado pasado **Guillermo les remarcó varias veces que jamás había estado en Bahía Blanca y que nunca había cometido un delito** ni tenía antecedentes penales.

"Dos policías se me acercan, me detienen, me piden el DNI y me dicen que los acompañe. Yo pensé que me iban a pedir que saliera de testigo de algo pero me dicen que quedaba demorado por una causa por robo agravado. **Me llevan detenido y pasaban los días y nadie me decía nada, nadie me explicaba nada**", contó.

"Me dicen que iba a quedar demorado porque tengo una causa en Bahía Blanca por robo agravado. Yo empecé a decir que nunca estuve ahí, me decían que sí y me tuvieron demorado desde el sábado hasta ayer, jueves, que me pareció muy raro. Yo quería que me llevaran lo más

El jueves un móvil policial lo fue a buscar para trasladarlo a una cárcel y en el camino llamó la fiscal del caso. "Se comunicó con los policías y **un jefe de ellos les dijo que me cuiden, que no me pase nada y preguntaron si iba esposado, que me saquen las esposas**", relató Ibarrola.

El hombre buscado por la Justicia era **Guillermo Walter Ibarrola**. Una persona con un nombre y número de DNI distinto.

"Ojalá que esto sirva para que no le pase a alguien como yo, que nunca cometí un delito, que nunca estuve detenido, **trabajé toda la vida pero me podrían haber arruinado la vida a mi y a mi familia**", insistió Ibarrola a la prensa.

Seguí leyendo:

[Detuvieron en Miami a un argentino acusado de tener pornografía infantil dentro de una guardería para niños](#)

TEMAS RELACIONADOS

Bahía Blanca retiro

ÚLTIMAS NOTICIAS

Agentes de inteligencia del Reino Unido creen que Rusia robó secretos de la fórmula de AstraZeneca para desarrollar la vacuna Sputnik V

Tras los rumores sobre la fuga de la fórmula británica sobre el tema, el ministro del Interior de Londres dijo que "hay estados extranjeros que constantemente quieren poner sus manos en información sensible, incluyendo secretos comerciales y científicos y propiedad intelectual"



Juan Manzur viajará a los Estados Unidos para reforzar el equipo que



ANEXO

VI



REPUBLICA ARGENTINA - MERCOSUR
REGISTRO NACIONAL DE LAS PERSONAS
MINISTERIO DEL INTERIOR, OBRAS PUBLICAS Y VIVIENDA



Apellido / Surname
CASTILLEJO ARIAS

Nombre / Name
PAULA

Sexo / Sex
F

Nacionalidad / Nationality
ARGENTINA

Ejemplar
B

Fecha de nacimiento / Date of birth
28 MAY / MAY 1997

Fecha de emisión / Date of issue
24 OCT / OCT 2016

Fecha de vencimiento / Date of expiry
24 OCT / OCT 2031

FIRMA IDENTIFICADO / SIGNATURE

Documento / Document

19.046.895

Trámite Nº / Of. ident.
**00461791689
9000**



DOMICILIO: FREIRE 4439 - CIUDAD DE BUENOS AIRES -
CIUDAD DE BUENOS AIRES - ARGENTINA
LUGAR DE NACIMIENTO: CARAGAS, VENEZUELA - -
Nº 2 BS AS - NATURALIZADO EL: 09 JUN 2016

Lie D. Rogelio Frigerio
Ministro del Interior O. Pub. y Vivienda

PULGAR

IDARG19046895<6<<<<<<<<<<<<<<<
9705283F3110245ARG<<<<<<<<<<<<<8
CASTILLEJO<ARIAS<<PAULA<<<<<<

DOMICILIO: CONESA 3997 - SAAVEDRA - CIUDAD DE BUENOS
AIRES - CIUDAD DE BUENOS AIRES
LUGAR DE NACIMIENTO: VENEZUELA - -
FECHA DE INGRESO AL PAIS: 07 MAY 1999
CATEGORIA DE INGRESO: Permanente
EXPEDIENTE: 27962002 DISPOSICION: 5822
FECHA DE RADICACION: 30 MAY 2002

CUL: 20-93772464-1

Lic. D. Rogelio Frigerio
Ministro del Interior O. Pub. y Vivienda

PULGAR

IDARG93772464<2<<<<<<<<<<<<<<<<<<<
5908145M3408076VEN<<<<<<<<<<<<<<<<<<<4
CASTILLEJO<RIVERO<<VICTOR<LEOP



REPUBLICA ARGENTINA - MERCOSUR
REGISTRO NACIONAL DE LAS PERSONAS
MINISTERIO DEL INTERIOR, OBRAS PUBLICAS Y VIVIENDA

EXTRANJERO

Apellido / Surname
CASTILLEJO RIVERO

Nombre / Name
VICTOR LEOPOLDO

Sexo / Sex
M Nacionalidad / Nationality
VENEZOLANA Ejemplar
B

Fecha de nacimiento / Date of birth
14 AGO / AUG 1959

Fecha de emisión / Date of issue
07 AGO / AUG 2019

Fecha de vencimiento / Date of expiry
07 AGO / AUG 2034

FIRMA IDENTIFICADOR SIGNATURE

V. Castillejo



Documento / Document

93.772.464

Trámite Nº / Of. ident.
00606226751
7579





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: ADHIERE COMO ACTORA AL AMPARO

FIRMADO ELECTRONICAMENTE 12/10/2021 08:32:22

CASTILLEJO ARIAS VICTOR ATILA - CUIL 20-19054367-7