INTERPONE ACCIÓN DE AMPARO COLECTIVO - SOLICITA MEDIDA CAUTELAR DE NO INNOVAR.

******;** con domicilio real en la calle ***
*** de la Ciudad Autónoma de Buenos Aires, Apoderado del Observatorio de Derecho Informático, con el patrocinio letrado del Dr. *** ***, Abogado, inscripto en el *** C.A.P.C.F, con domicilio electrónico *** constituyendo domicilio procesal en calle *** de la Ciudad Autónoma de Buenos Aires correo electrónico ***t a V.S. me presento y respetuosamente digo:

I. PERSONERÍA.

Conforme surge de la copia del poder que acompaño al presente (Anexo I) el cual declaro bajo juramento que se encuentra vigente, el OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.) Asociación Civil debidamente inscripta en el Registro Público de Comercio de la Inspección General de Justicia bajo el número 213, del libro 2AC de Asociaciones Civiles (Anexo II), me ha conferido poder para representarla en estas actuaciones. En base a ello, solicito se me tenga por presentada y por acreditada personería.

II. OBJETO.

Que vengo por este acto, en legal tiempo y forma, a interponer acción de amparo en los términos del art 43 de la CN y la Ley Nº 2.145 de la Ciudad Autónoma de Buenos Aires, contra el Gobierno de la ciudad de Buenos Aires por encontrarse afectados derechos en el acto administrativo Resolución N° 398/MJYSGC/19 y en la Ley Nº 6.339, que modifica la Ley N.º 5.688 los artículos 478, 480, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis, por ser dicho acto y dichas modificaciones inconstitucionales y contrarias a los distintos Convenios Internacionales firmados por el País, las mismas son con respecto al el Sistema de Reconocimiento Facial de Prófugos , el Sistema Preventivo y

el Sistema Forense, sus correspondientes Registros de Base de Datos Informatizada y de la que se realizan tratamientos de datos automatizados, El sistema de Borrado o Conservación de imágenes y videos, los plazos para remitir informaciones, modificaciones y criterios en cuanto la implementación de el sistema por parte de la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia y Defensoría del Pueblo por no existir los informes Constitucionales y Convencionales previos, así como la conformación de la propia Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia, a fin de que se realice un control de constitucionalidad y convencionalidad de dichos acto administrativo y dichos artículos en las leyes mencionadas.

La afectación de nuestros Derecho Constitucionales se encuentran enumerados en los artículos 14, 14 bis 18, 19, 33, 43, 75 inc 22; artículos 14, 16, 18, 34, 36, 38, 39, 61 de la Constitución de la Ciudad Autónoma de Buenos Aires, en la OC 5/85 de la CIDH (Derecho a Reunión de Terceros), art 1710 del CCCN, Pacto de San José de Costa Rica artículo 7, Pacto de Derechos Civiles y políticos en sus artículos 4, 5, 7, 9, 14, 17, 20, 21, 24, ley Nº 2.145 de la Ciudad Autónoma de Buenos Aires, Ley Nº 1845 de CABA sobre protección de datos personales, Ley Nº 25.326 de Protección de Datos Personales, Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y protocolo adicional al convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos de datos transfronterizos, procurandosé con ésta acción la tutela jurisdiccional frente a la conducta ilegítima y arbitraria del Estado de la Ciudad Autónoma de Buenos Aires, Ley Nº 5688.

Asimismo y como medida cautelar, vengo a solicitar se proceda inaudita parte a dictar la medida cautelar de no innovar establecida en el art. 15 de la Ley Nº 2.145 y concordantes a fin de que V.S. ordene la inmediata suspensión sobre el acto administrativo Resolución N° 398/MJYSGC/19 y los siguientes artículos de la Ley Nº 6.339 que modifica la ley Nº 5.688 en sus artículos 478, 480, 483, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis, a fin de evitar los graves perjuicios que la aplicación inmediata de estos artículos provoca, conforme a las consideraciones de hecho y derecho que seguidamente expongo:

III. LEGITIMACIÓN.

1. Nos encontramos legitimados activamente para entablar la presente demanda puesto que toda la sociedad en su conjunto ha sido alcanzada por los efectos de la promulgación de la Ley Nº 6.339 que modifica los artículos mencionados UT SUPRA de la Ley Nº 5.688 y el acto administrativo de la Resolución N° 398/MJYSGC/19 que lesionan de forma manifiesta los derechos de toda la sociedad.
2. Que el OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.) se encuentra legalmente registrado para ejercer acciones judiciales en carácter colectivo.
3. Que el artículo 14 de la Constitución de la Ciudad Autónoma de Buenos Aires se encuentra establecida la acción de amparo en concordancia al artículo 43 de la Constitución Nacional.
4. Que la Ley Nº 2.145 regula dicha acción y en su artículo 7º establece que el fuero competente es el Contencioso Administrativo y Tributario de la Ciudad Autónoma de Buenos Aires por ser contra las autoridades públicas de la Ciudad.
5. Tanto el art 43 segundo párrafo y el art 14 de la Constitución local, enumeran derechos colectivos, sin que esa clasificación pueda ser considerada en modo alguna como taxativa, por el contrario debe ser vista como la ejemplificación de algunos y más comunes derechos de incidencia colectiva, que no agotan su esfera en el texto constitucional, sino que se actualizan y recrean.

   Los derechos colectivos, entendidos como derechos fundamentales “comparten el mismo ámbito de aplicación que los derechos fundamentales subjetivos y persiguen el mismo fin: dotar a la persona de identidad normativa y simbólica, tanto en su faz individual frente al Estado y a las demás personas, como en su faz de integración solidaria a un ente colectivo frente al Estado y a las demás personas... Los derechos colectivos adscriben a una visión de la persona que se sitúa más allá de su individualidad y se ubica en torno a la solidaridad... La posibilidad de que los seres humanos demanden derechos colectivos sólo puede fundarse bajo el supuesto de que lo social y lo individual integran la realidad de toda persona y que es posible mantener razonablemente y constatar que, además de una vida individual, hay una vida colectiva (distinta de la individual aunque no absolutamente separada) que se constituye mediante relaciones interindividuales en el marco de una coexistencia y convivencia de individuos concretos” (cfr. Gil Domínguez, Andrés, Neoconstitucionalismo y derechos colectivos, Editorial Ediar, Buenos Aires, 2005, pág. 133/135).

> La Corte Suprema de Justicia de la Nación en el caso “Halabi”, ha delimitado tres categorías de derechos: individuales, de incidencia colectiva que tienen por objeto bienes colectivos, y de incidencia colectiva referentes a intereses individuales homogéneos. En todos ellos considera imprescindible la existencia de “caso”. Menciona allí tres elementos relevantes en los derechos de incidencia colectiva referidos a intereses individuales homogéneos: a) la existencia de un hecho único o complejo que causa una lesión a una pluralidad relevante de derechos individuales; b) la pretensión debe estar concentrada en los efectos comunes y no en lo que cada individuo puede peticionar; y c) se exige que el interés individual considerado aisladamente, no justifique la promoción de una demanda, con lo cual podría verse afectado el acceso a la justicia.

En la presente acción hay un hecho, único o continuado, que provoca la lesión de todos ellos y por lo tanto es identificable una causa fáctica homogénea... Hay una homogeneidad fáctica y normativa que lleva a considerar razonable la realización de un solo juicio con efectos expansivos de la cosa juzgada que en él se dicte, salvo en lo que hace a la prueba del daño”. (C.S.J.N., “Halabi, Ernesto c/P.E.N., ley 25.873 dto. 1563/04), 24/02/2009, La Ley 02/03/09).

PROCEDENCIA DE LA ACCIÓN DE AMPARO - PRESUPUESTOS DE ADMISIBILIDAD.

El artículo 43 CN establece requisitos de procedencia de la acción de amparo, los que se encuentran debidamente cumplidos en la presente causa, a saber:

1) Existe un acto de autoridad pública: En forma primera fue realizada una contratación directa del Gobierno de la Ciudad Autónoma de Buenos Aires a una Empresa Privada y de forma posterior se sancionó la Ley Nº 6.339 donde se proponen modificaciones a la ley Nº 5.688 dando origen al acción de Amparo aquí presentado.

2) Que en forma inminente amenace o restrinja: dicha ley afecta nuestros Derecho Constitucionales enumerados en los artículos 14, 14 bis 18, 19, 33, 43 75 inc 22; artículos 14, 16, 18, 34, 36, 38, 39, 61 de la Constitución de la Ciudad Autónoma de Buenos Aires, en la OC 5/85 de la CIDH (Derecho a Reunión de Terceros), Pacto de San José de Costa Rica Artículo 7, Pacto de Derechos Civiles y políticos en sus artículos 4, 5, 7, 9, 14, 17, 20, 21, 24. Convenio 108 del Consejo de Europa ratificado por Argentina, Ley Nº 1845 Datos Personales CABA, Ley Nº 25.326 Datos Personales, Resolución 1/2015 ONTI.

3) Conculca con ilegalidad y arbitrariedad manifiesta derechos fundamentales y garantías reconocidas por la CN y los instrumentos internacionales sobre derechos humanos con

jerarquía constitucional: Cuando las disposiciones de esta ley que se tacha de falta de control convencional y de tratados internacionales en la presente acción, claramente no respetan los preceptos constitucionales, la arbitrariedad e ilegalidad es manifiesta.

4) En cuanto al recaudo: “medio judicial más idóneo”, no es un acto muy complejo establecer que para la situación planteada, no existe un remedio judicial alternativo que sea expedito, rápido y que, garantizando una decisión oportuna de jurisdicción, resguarde los derechos fundamentales conculcados. Estamos ante una cuestión de pleno derecho, donde no es necesario un amplio debate o la producción de prueba. En este sentido, pensemos que consecuencias traería la utilización de la vía ordinaria, aún en el supuesto de alcanzar una sentencia de primera instancia favorable: un proceso lento y engorroso que podría durar años y que se devoraría la pretensión procesal.

5) La ostensible inconstitucionalidad de estas modificaciones, cuya declaración se persigue mediante esta acción de amparo, es cuestión judiciable.

En nuestro ordenamiento jurídico, artículo 31 CN, la voluntad del Constituyente prima sobre la del Legislador, por lo que, atento las facultades de control de constitucionalidad de las leyes confiado por la CN al Poder Judicial, corresponde que éste intervenga cuando tales derechos se desconozcan o se encuentren amenazados.

IV- HECHOS.

El sistema de reconocimiento facial de prófugos: En fecha 3 de abril de 2019, se realizó el “Primer Congreso Internacional de Delito Transnacional” que se llevó a cabo en la Legislatura Porteña. En dicha oportunidad, el Ministro de Justicia y Seguridad de la Ciudad, el Sr. Mtro. Diego Santilli anunció la implementación de un nuevo sistema de reconocimiento facial (de ahora en más “SRFP”) que funcionaría también con “Inteligencia Artificial”.

Asimismo, el Sr. Mtro. manifestó que dicho sistema se encontraría operacional en algunas semanas posteriores.

Esto motivó ciertos reparos por parte de la ciudadanía, las Asociaciones Civiles y demás organizaciones, e inclusive por la misma Defensoría del Pueblo de CABA, quien le envió el correo electrónico que se acompañó como Anexo III al suscripto. Todos ellos expresaron sus miedos a que con el uso de esta nueva tecnología se violara la privacidad, intimidad y datos personales de las personas.

No obstante, en fecha 25 de abril de 2019 con la publicación de la Resolución Nº 398/2019 (de ahora en más “Resolución 398”) de manera totalmente intempestiva, nos enteramos que este sistema de reconocimiento facial fue implementado.

La puesta en funcionamiento del SRFP fue totalmente sorpresiva.

Los sistemas de reconocimiento facial (SRF) funcionan mediante la comparación de características biométricas de dos rostros. Para poder llevar a cabo esta tarea, deben aprender cuándo se trata de la misma persona y cuándo no. Esto lo logran a partir de una base de datos de distintas caras y mediante una “Carga” de información constante, sin tener en cuenta la base de datos biométricos a la cual contrastar, por el contrario esa base es la “memoria” para mejorar el funcionamiento de la Inteligencia Artificial y no hace diferencias entre la base de datos de la CONARC sino que toma la totalidad de rostros que pasen por la Cámara.

Si uno analiza la aplicación de este tipo de sistemas en otras capitales del mundo observa que fueron precedidas de un amplio y fuerte debate por parte de la ciudadanía y las autoridades gubernamentales. Así se debatió acerca de la posible afectación de datos personales y si la implementación de cámaras de video vigilancia con sistemas de reconocimiento facial contribuye o ha contribuido a la mejora de la seguridad pública. Más allá que en algunos casos ha resultado justificable y en otros cuestionable, en aquellos países donde se terminó aplicando el sistema, la justificación del sistema, su legitimidad, necesidad y proporcionalidad se estableció mediante una “evaluación del impacto en la privacidad” (“Privacy Impact Assessment”).

La Evaluación de Impacto en la Privacidad (EIP) o Privacy Impact Assessment (PIA) en sus siglas inglesas, constituye una serie de métodos mediante los cuales se evalúan los riesgos que un producto o servicio conlleva sobre la privacidad de los datos personales que maneja. Esta evaluación previa –que suele ser realizada por el propio gobierno para los casos de implementación de sistemas que operan en el espacio público con registros públicos - permite la correcta gestión de los riesgos antes de su aparición y la implantación de las medidas que permitan eliminarlos o mitigarlos.

Esta evaluación no fue realizada por el GCBA y, a la fecha, no es posible determinar el impacto y la posible afectación a los datos personales y otros derechos humanos básicos de los ciudadanos de la CABA, por parte del sistema implementado.

Por esta razón, desde O.D.I.A. se presentó un pedido de información en fecha 4 de julio de 2019 el cual acompañamos como Anexo IV y pasamos a detallar:

1- La solicitud de información pública:

Dicho pedido está compuesto por 77 preguntas. Las primeras 75 están destinadas a:

(i) conocer cierta información sobre el proceso mediante el cual se licitó el SRFP;

(ii) a conocer los antecedentes de la Resolución 398 mediante el cual se implementó el sistema;

(iii) a averiguar si el GCBA tenía los protocolos correctos de seguridad de la información;

(iv) conocer los resultados del uso del SRFP en estos primeros meses;

(v) conseguir copia de cierta documentación importante;

(vi) conocer los antecedentes administrativos previos a su implementación.

Por el otro lado, las últimas 2 preguntas (76 y 77) están destinadas algunas cuestiones puntuales acerca del "Pliego de Especificaciones Técnicas del Servicio de Análisis Integral de Video" (de ahora en más "el Pliego") mediante el cual el propio gobierno de la Ciudad Autónoma de Buenos Aires expuso los requisitos técnicos que quería que el SRFP tuviera.

Como veremos en los párrafos siguientes todas las preguntas realizadas por nuestra parte están absolutamente autorizadas por la normativa y no entran dentro de las excepciones previstas en el art. 6 de la Ley 104.

Asimismo, una vez realizada la presentación a través del portal específicamente provisto por el GCBA para ello, nos enviaron los mensajes de correo electrónico que acompaño como Anexo V y VI.

Mediante el primero, el GCBA nos hizo saber que dentro de las 48 horas hábiles se iba a estar verificando que nuestra solicitud correspondía efectivamente a un pedido de acceso a la información pública. Además, se nos hizo saber que el número de expediente de nuestro pedido pasaría a ser "00912237/19", que con la segunda respuesta pasaría a ser "GENERO EX-2019-21385378- -GCABA- DGSOCAI".

Mediante el segundo número de expediente, en fecha 27 de agosto de 2019, 15 días después del tiempo estipulado el MJYSGC respondió en forma incompleta, parcial y deficiente a nuestras preguntas.

2- La respuesta del MJYSGC.

Antes de analizar pormenorizadamente las omisiones en la contestación brindada por el MJYSGC, corresponde hacer notar que el tema objeto de esta acción es sumamente complejo y técnico. La Sociedad Civil organizada en Asociaciones similares a O.D.I.A. hace enormes esfuerzos para controlar y contrarrestar las acciones que podrían traducirse en una eventual o inminente afectación de derechos a gran escala por ser realizadas por parte del estado. Por ende, cuando estas asociaciones realizan pedidos de información a las entidades gubernamentales, estas deben ser contestadas con la suficiente seriedad y dedicación ya que de lo contrario, se debilitaría el sistema democrático y los principios republicanos que garantizan la publicidad de los actos de gobierno y el control por parte de los ciudadanos de dichos actos y la responsabilidad de los funcionarios por los actos que realizan en el marco de sus funciones.

Como dijimos anteriormente, la respuesta del MJYSGC fue recibida en el correo electrónico odiaasoc@gmail.com en fecha 27 de agosto de 2019, el mismo lo adjuntamos como Anexo VII. En dicho correo electrónico se adjuntaron 2 archivos PDF donde se encontraría la información solicitada por mi parte (Anexo VIII y IX).

El Anexo VIII parece ser una respuesta genérica mediante la cual el Ministerio intenta dar por satisfecho el pedido de información. El párrafo que más nos llamó fue el siguiente: “Los considerandos del acto y el anexo operativo que lo acompaña (IF-2019-12925085-GCABA-MJYSGC también de carácter público) dan respuesta a la totalidad de los puntos que contiene el extenso cuestionario presentado, en todo aquello que corresponde a la competencia funcional de esta Secretaría de Justicia y Seguridad, en tanto sea calificable como “información pública” y no se dirija simplemente a inquirir sobre el giro ordinario de los asuntos de gestión, aspecto ajeno a tal concepto de conformidad con pacífica doctrina judicial y administrativa.”

Desde ya negamos que dicha providencia pueda ser considerada como respuesta a la preguntas formuladas y sostenemos que únicamente la NOTA nro. NO-2019-25581723-GCBA-DGEYTI, debe ser el acto a revisar para determinar se ha sido satisfecho el pedido de acceso a la información.

Dicho esto, pasaremos a analizar la NOTA nro. NO-2019-25581723-GCBA-DGEYTI. Asimismo, hacemos la aclaración de que la Ley 104 no presupone la necesidad de que quien solicita la información tenga que explicar la razón por la cual solicita dicha información, pero, haremos referencia a algunas preguntas:

D.1. Preguntas que damos por contestadas.

En primer lugar, a efectos de no extendernos más de la cuenta, damos por contestadas las preguntas número 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 14, 43, 49, 55, 56 y 66.

D.2. Preguntas con respuestas parciales que no satisficieron el pedido de información.

Por el otro lado, hay un número de preguntas que, si bien se "contestaron" (en el sentido de que aparentan tener una respuesta), lo cierto es que o, no "contestaron" lo que se estaba preguntando o directamente omitieron información que hacía a la esencia de la pregunta que se estaba realizando.

Entendemos que el acceso a la información pública de manera completa, clara y veraz hace a la esencia de los derechos de la ciudadanía civil. Esta información le permite a la misma intentar mantener a raya los abusos que pueda llegar a realizar la administración y controlar que todos sus actos sean acordes a la normativa aplicable.

Por esta razón, la legislatura de la Ciudad ha promulgado la Ley 104 mediante la cual se establecieron principios que los organismos estatales deben respetar a efectos de cumplir con la manda de los ciudadanos de la ciudad. Entre esos principios se encuentran el de máxima premura; presunción de publicidad y accesibilidad; informalismo; no discriminación; eficiencia; completitud; disociación; transparencia; formatos abiertos; alcance limitado de las excepciones; in dubio pro petitor; buena fe y gratuidad.

No obstante lo anterior, y como veremos a continuación, el Ministerio se dedicó a empantanar, obscurecer, dificultar y directamente omitir la entrega de la información requerida por mi parte:

Preguntas Nº 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?-.

El GCBA contestó: "Por una cuestión de seguridad informática no es posible brindar esa información". Lo cierto es que el art. 6 de la ley de Acceso a la Información no prevé a la "seguridad informática" como supuesto para eximirse de brindar la información requerida.

Por otro lado, es de señalar el hecho de que, atento a los principios reseñados anteriormente, mal podría la administración exceptuarse del cumplimiento de sus obligaciones en relación al Derecho de Acceso de O.D.I.A. mediante la mera invocación de un principio abstracto.

Pregunta N° 21:) Informe si el software reconoce a menores de edad.

Si bien se contesta que el software no reconoce menores de edad, lo cierto es que no explica de qué manera se llega a esa conclusión, ya que no solo lo solicita directamente en el Pliego sino también que la razón indicaría que para determinar esa respuesta, el software en algún momento debería reconocerlos.

Preguntas 22) ¿Qué información se registra y archiva acerca de ellos? y 23) ¿Con quién se comparte dicha información y con qué fines?

El GCBA responde “N/A”. ¿Acaso debemos inferir que se trata de la abreviatura de uso común en el inglés, utilizada para indicar que la información requerida no está disponible (not available)? Claramente la respuesta no cumple con lo normado por el art. 5 de la Ley de acceso a la información, que obliga al requerido a “informar los motivos por los cuales no la posee”.

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

No indicó si efectivamente existía algún convenio.

Pregunta 44: ¿En qué tipo de aparatos reciben las alertas generadas por el sistema los agentes de la Policía? ¿En qué momentos los agentes destruyen aquellos archivos que le fueron enviados a esos aparatos? ¿Qué sistema o 8 protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos y como se audita su correcta destrucción?.

El GCBA no explica que es un POC ni tampoco indica que tipo de aparato es utilizado. Se limita a establecer que es un “teléfono institucional” pero no indica que tipo de teléfono, marca, características, etc.

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

No indica que información es efectivamente remitida a los agentes de la policía y tampoco explica que sistema es utilizado para la remisión de esa información. No explica a que se refiere con “APK”.

Pregunta 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 GCBA omite totalmente responder la pregunta.

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

El GCBA se limitó a manifestar que el índice de precisión era del 95% (y que desde ya negamos que eso sea así), sin establecer expresamente cuantos falsos positivos podía generar el SRFP.

Pregunta 61, 62 y 68:

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?.

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

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.

El GCBA dice que la información estaría protegida por “copyright” y que por esa razón no tienen acceso. Esta información es totalmente indispensable a efectos de determinar la seguridad y/o confiabilidad del SRFP. Nuestra pregunta no está dirigida a determinar secretos comerciales ni derechos protegidos por la propiedad intelectual. Solicitamos en términos conceptuales se nos indique que método de detección de rostros se utiliza, sin especificar absolutamente nada más que el método. Por el otro lado, cuando nos referimos a el set de datos para entrenar el modelo nos referimos a las imágenes utilizadas para entrenarlo ya que si utilizaron imágenes de otros países con otras idiosincrasias, la probabilidad de que ocurran falsos positivos es mucho más alta. No obstante, adelantamos que si dudas hay acerca de la protección que se le debe dar a este sistema.

Pregunta 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?.

La pregunta estaba dirigida a averiguar a qué porcentaje de confiabilidad en una coincidencia se había comprometido la empresa y además a que indicará que porcentaje de efectividad se ha comprometido.

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

Se utilizan términos como SLA que mi parte desconoce. Además insinúa que hay otros procesos de control que no nos ha mencionado.

Pregunta 67: ¿Se ha hecho una auditoría del software por un tercero independiente?.

La pregunta estaba dirigida ha si ya se había hecho una auditoría del software. El GCBA se limita a decir que la autoridad encargada de esa auditoría era la defensoría del pueblo.

Preguntas Nº 76 y 77:

76) 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?.

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”?

El GCBA se limitó a pegar un link al pliego de las bases y condiciones para la contratación del SRFP que mi parte ya ha analizado exhaustivamente y que motivaron expresamente las preguntas realizadas. Adjuntamos para la consideración de V.S. el pliego de bases y condiciones como Anexo IX.

La contestación del GCBA se limitó a alegar “seguridad informática” (respuesta a satisfactoria y suficiente y, por ende, determinar que esa información fuera sustraída del acceso irrestricto de la ciudadanía.

En tales condiciones, resulta aquí aplicable la rigurosa expresión afirmada por la Corte Suprema de Justicia de la Nación en un caso que guarda suficiente analogía con el presente, de que: "Convalidar, sin más, una respuesta de esa vaguedad significaría dejar

librada la garantía del acceso a la información al arbitrio discrecional del obligado y reduciría la actividad del magistrado a conformar, sin ninguna posibilidad de revisión, el obrar lesivo que es llamado a reparar" (Fallos: 338:1258, considerando 27).

D. 3. Preguntas no contestadas, cuya omisión no fue justificada ni fundada.

A continuación, enumeramos las preguntas que no fueron contestadas y explicamos la importancia de contar con la información requerida:

Pregunta Nº 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?.

la información solicitada es necesaria a los fines de poder determinar si ha existido o existe una Evaluación de Impacto en la Privacidad (EIP) respecto del sistema de reconocimiento facial.

Pregunta Nº 13: ¿Qué técnica de borrado es utilizada? ¿Cómo se audita y de qué manera se asegura que las imágenes son efectivamente eliminadas?.

No se respondió acerca de qué manera es realizada la auditoría del borrado de las imágenes, ni tampoco cuál es la técnica de borrado utilizada.

Preguntas Nº 16 y 17:

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:

16) ¿Qué tipos de tareas pueden ser requeridas por el Ministerio Público Fiscal, el Poder Judicial de la Nación, Provincial y de la Ciudad Autónoma de Buenos Aires?.

17) ¿Qué se quiso decir con “(…) 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) (…)”? ¿No es el principal objetivo de este sistema el

Reconocimiento Facial de Prófugos? ¿De no ser así, que otros objetivos se tuvieron presente para la implementación de este sistema?.

No fue contestado para cuáles otras tareas puede ser utilizado el SRFP, cuando supuestamente, el único objetivo del sistema era la detección de prófugos.

Preguntas Nº 18, 19 y 20:

18) ¿En qué contexto se pueden incorporar imágenes al sistema de personas que no se encuentran registradas en el CONARC?

19) ¿Qué quiere decir "(…) salvo orden judicial (…)? ¿Oficio con firma de juez?

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

La información requerida resulta necesaria para evaluar la seguridad del sistema.

Preguntas Nº 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, y 36:

26) ¿A qué requerimiento se refiere la última parte del art. 3? ¿Por qué este requerimiento tiene que estar dirigido a la Secretaría de Justicia y Seguridad? El art. 4 del Anexo también establece que "[…] El personal que sea autorizado por este Ministerio de Justicia y Seguridad para la operación y acceso al Sistema de Reconocimiento Facial de Prófugos, deberá suscribir el correspondiente convenio de confidencialidad, en la forma que determine la Secretaría de Justicia y Seguridad." En virtud de lo dispuesto por este artículo solicitamos se nos informe:

27) ¿En qué consiste la autorización que realizaría el Ministerio de Justicia y Seguridad al personal que tendría acceso y operaría este nuevo Sistema de Reconocimiento Facial?

28) Solicitamos copia íntegra (en formato digital que podrá ser enviado al correo señalado en el encabezado) del convenio de confidencialidad que sería firmado por el personal que operaría el sistema.

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

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

31) De existir civiles autorizados, ¿Qué rol cumplen en la operatoria del Sistema y por qué es necesario que estos tengan acceso? En el último párrafo del art. 5 del Anexo se establece

lo siguiente: “[…] La Policía de la Ciudad no está autorizada a ceder tales archivos a ninguna otra autoridad administrativa de la Ciudad, con excepción del Ministerio de Justicia y Seguridad el que tampoco podrá utilizarlos para finalidades distintas a aquéllas que motivaron su obtención.”

32) ¿Por qué razón los archivos generados por el Sistema pueden ser cedidos al Ministerio de Justicia y Seguridad?

33) Si bien la Policía de la Ciudad no se encuentra autorizada a ceder los archivos a ninguna otra autoridad administrativa ¿Pueden ser cedidos a una autoridad de otro tipo?

34) ¿Pueden ser cedidos a otro organismo de las Provincias, del gobierno nacional o alguna otra entidad judicial? ¿Por qué razón?

35) ¿Pueden ser cedidos a otras fuerzas de seguridad?

36) ¿Qué motivos pueden justificar que dichos archivos sean cedidos al Ministerio de Justicia y Seguridad?

la información solicitada es necesaria a los fines de poder determinar si ha existido o existe una Evaluación de Impacto en la Privacidad (EIP), si se puede determinar si se protegerá adecuadamente la información acumulada por este SRFP, entre otras cuestiones.

Preguntas Nº 37, 38, 39, 40, 41, 42, 46, 47 y 48:

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?

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

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

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

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

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

46) ¿Qué policías reciben esta información?

47) ¿cuántos agentes reciben esta información?

48) ¿En qué consisten estas alertas?

La información requerida resulta necesaria a los fines de evaluar el uso de los resultados del sistema por parte de la autoridad de prevención y asimismo determinar si existen protocolos de actuación por parte de las fuerzas de seguridad en casos de "falsos positivos".

Preguntas Nº 50 y 51:

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?

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?

A los fines de evaluar la "performance" del sistema resulta imperioso saber el número de aciertos (personas detenidas por pedidos de detención vigente) y el número de "falsos positivos".

Preguntas Nº 52 y 53:

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.

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"?

Conforme lo expuso el Relatos de las Naciones Unidas en el documento ofrecido como prueba, contar con una definición de "delito grave" a los fines de ser utilizado como

criterio delimitar resulta imperioso a los fines de determinar el universo de personas que conforman la lista/registro que posee el sistema.

Preguntas Nº 54, 57 y 58:

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?

57) ¿Qué tipo de contrato se ha firmado? Se solicita copia de este en soporte digital enviado a la dirección de correo electrónico señalado en el encabezado.

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

La información requerida es necesaria a los fines de conocer la empresa que obtuvo la licitación y si existe un protocolo que proteja la información sensible de las personas que figuran en la lista, en caso de que la firme deje de existir. Asimismo, se necesita a efectos de evaluar la posible ocurrencia de hechos contrarios a lo dispuesto por la Ley de Compras y Contrataciones de la Ciudad.

Pregunta Nº 64:

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

Es necesario conocer si existe un control por parte de la Ciudad, acerca de los compromisos asumidos por la empresa.

Requisitorias Nº 25, 69, 70, 71, 72, 73, 74 y 75: no fueron contestadas ni enviados los documentos solicitados, ni justificada dicha omisión.

25) De existir dicho convenio, se solicita copia del mismo en soporte digital al correo electrónico establecido en el encabezado.

69) Copia del expediente EX-2019-12872444- -GCABA-SECJS.

70) Copia de la nota N° NO-2019-08826279-SECJS mediante la cual el Secretario de Seguridad y Justicia requirió la contratación directa.

71) Copia de la Nota N° NO-2019-09163643-DGEYTI de la Dirección General Estudios y Tecnologías de la Información determinó como oportuna la contratación directa en virtud de lo dispuesto por el Art. 28 inc 6 de la Ley N° 2095.

72) Copia de cualquier otro pedido de información relacionado con el sistema de reconocimiento facial de prófugos implementado y el que deberá tener anexado la correspondiente respuesta (Si la misma existe).

73) Copia del Pliego de Bases y Condiciones, resolución de adjudicación, y cualquier otra Resolución, Disposición, Reglamento o norma relacionado con el uso de este nuevo Sistema de Reconocimiento Facial de Prófugos.

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.

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

El hecho de que el GCABA haya omitido dar respuesta sin siquiera haber justificado tal omisión constituye una palmaria afectación al derecho de todo ciudadano de acceder a la información pública, máxime cuando se tiene en consideración que la información requerida se vincula a un sistema cuya aplicación puede afectar y vulnerar a gran escala, derechos de entidad constitucional.

Resta señalar que, la carga de la prueba de la legitimidad de la restricción corresponde al Estado (conf. CIDH, Caso "Claude Reyes", antes citado, párrafo 93), y que cuando se deniega una solicitud de información debe hacerse mediante una decisión escrita,

debidamente fundamentada, que permita conocer cuáles son los motivos y normas en que se basa para no entregar la información en el caso concreto (Fallos: 335:2393, considerando 9 °; y 338:1258, considerando 7°; también CIDH, Caso "Claude Reyes", párrs. 77 y 158).

El silencio no es una opción para el Estado.

A razón de ello se inició un acción de amparo a los fines de que brinde en debida forma el pedido de acceso a la información relacionado con la resolución 398/MJYSGC/2019, dicha causa tramita en el Juzgado de primera Instancia en lo Contencioso administrativo y Tributario N.º 23 secretaria N.º 45 expte 9480/2019-0, el cual su estado procesal se encuentra con sentencia de primera instancia favorable a ésta parte, con la apelación respectiva del gobierno de la ciudad, a la fecha dicho expte se encuentra a la espera de una sentencia en segunda instancia.

El 19 de noviembre del año 2020 se publica las modificaciones a la Ley Nº 6.339, que modifica la Ley N.º 5.688 los artículos 478, 480, 480, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis, resultando ser las mismas inconstitucionales conforme lo expuesto hasta aquí y conforme se indica en el punto V de este escrito de inicia.

IV.a. La implementación del SRF (Sistema de Reconocimiento Facial) en la CABA.

La implementación del SRF en la CABA ha tenido un desarrollo sinuoso e inusual. El sistema, en su primera etapa como ya hemos indicado, fue anunciado por el Sr. Vicejefe de gobierno, Diego Santilli, el día 3 de abril de 2019 durante la celebración del Congreso Internacional sobre delito Transnacional [1]. En tal oportunidad, el referido funcionario político, estableciendo plazos de imposible cumplimiento según la bibliografía en la materia, indicó que el sistema a implementar se encontraría operativo a partir del día 22 del mismo mes.

Tal anunció obedeció al hecho de que el mismo día del anuncio, a las 19:02hs, fue publicado el Pliego de Bases y Condiciones Particulares para la Contratación Directa de un Servicio de el Análisis Integral de Vídeo (de aquí en adelante “el Pliego) bajo PLIEG-2019 - 10400885 - GCBA - SSGA. Seis Minutos más tarde, con una celeridad realmente envidiable, el citado pliego resultó autorizado por las autoridades intervinientes por

1https://www.telam.com.ar/notas/201904/346605-sistema-de-reconocimiento-facial-ciudad-abril.html

mediante la suscripción de la Resolución 2019-59- GCBA-SSGA. Este derrotero administrativo llevado en plazos poderosamente llamativos para los estándares usuales, se vería finalizado pocos días después por medio de la suscripción de la Resolución 2019-98-GCBA-SSGA, de fecha 22 de abril de 2019, mediante la cual fuera aprobada la Contratación Directa N° 2900-0472-CDI19. Finalmente, el flamante sistema comenzó a operar en la vía pública porteña el día 25 de abril de 2019[2]

Lo relatado da cuenta a primera vista de lo inusual y hasta ilógico de los plazos transcurridos para la implementación de este sistema de carácter crítico. Tal realidad surge de modo palmario al tomar en consideración la circunstancia de que, desde la publicación de los respectivos pliegos, la puesta en funcionamiento del sistema, solo tomó 22 días corridos.

Este hecho, lejos de circunscribirse a un ejercicio de cronometría de la administración pública, permite vislumbrar el hecho de que la referida implementación resultó una llevada a cabo en franca contradicción con las prácticas y tiempos habituales del rubro informático para tareas de esta naturaleza. Por otro lado, el sistema de reconocimiento facial de prófugos de la ciudad reconoce una segunda en su implementación a partir de la sanción del acto administrativo de la Resolución N° 398/MJYSGC/19 de la Ley Nº 6.339, que modifica la Ley N.º 5.688 los artículos 478, 480, 480, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis, dicho sistema y modificaciones son inconstitucionales conforme lo que expresamos en el punto V.

Sea resultado de esta imposibilidad de implementar un sistema de estas características en el plazo descrito, que el cúmulo de falencias e irregularidades detectadas surgen de modo palmario y ostensible conforme se detalla aquì en èste punto y a lo largo de este escrito de inicio: Crea falsos positivos, es decir elige a personas con similares características dando datos erróneos de alertas, el SRFP tiene un efectividad que se encuentra por debajo del 50%

La base de datos del CONARC posee errores, la Dirección Nacional del Registro Nacional de Reincidencias el 6 de noviembre del 2019, indicó mediante disposición 7/2019 que del CONARC se permitió advertir que la existencia de casos de rebeldías, órdenes de captura etc, lo habían sido sin relacionar a la persona imputada no comparecida con número de DNI alguno, fuere nacional o extranjero

“Una prueba en la ciudad de Nueva York arrojó datos preocupantes porque el grado de eficacia fue cero. En Estados Unidos se utilizó para identificar a los

2 https://www.clarin.com/policiales/ponen-marcha-rastreo-profugos-sistema-reconocimiento-facial_0_OGE78UGxS.html

automovilistas que cometían infracciones y el fracaso fue rotundo. Algo parecido ocurrió en Londres, con una tasa de error del 98% "(Fuente www.perfil.com).

"San Francisco, uno de los principales polos tecnológicos del mundo, busca prohibir este software. Es la primera ciudad que le planteó una guerra a esta herramienta: la Junta de Supervisores votó la ordenanza para detener la vigilancia secreta (SSSO). En Europa, este mismo sistema fue testeado en un partido de fútbol con el objetivo de identificar a los espectadores. El grado de eficacia fue del 8%. Perdieron por goleada." (Fuente www.perfil.com).

IV.b1. Las Deficiencias del SRF y las consecuentes contradicciones del GCBA.

Como pudimos observar en el raconto de los hechos en ningún momento el GCBA puede contestar las preguntas que deberían haberse realizado y ésto no es menor para la sociedad en su conjunto, dado que la imposibilidad de no detectar personas menores de edad, no indicar cómo "aprende" el sistema deja en completo descubierto el sesgo racial y de género con el que ya viene pregonando absolutamente todos los sistemas de reconocimiento facial a lo largo y ancho del planeta, motivos por los cuales se dejó de utilizar y siempre en respeto de las minorías raciales y de género.

IV.b.2 Observación Efectuada por el Relator Especial de la ONU.

Por el cual manifiesta su honda preocupación de que no hayan realizado ninguna evaluación de impacto en la privacidad antes de implementar amplias redes de cámaras de vigilancia o sistemas de reconocimiento facial y reconocimiento de matrículas

IV.b.3 Contradicción Plazos de entrenamiento/contratación.

Todo sistema de identificación necesita que se le "cargue" información y esa no es menos que los datos biométricos que debe ir identificando, pero también se encuentra tomando e identificando la totalidad de los datos biométricos de quienes transitan bajo el lente de las cámaras de identificación biométricas devenidas en identificadoras de prófugos de la justicia a modo de un edulcorante que no deja de hacer un daño irreparable en la sociedad toda al no poder indicar cómo es que se entrena y el tiempo de contratación para el cual fue puesto en marcha de forma irregular y que la Legislatura intenta continuar con

la sangría de datos biométricos de sus ciudadanos a manos de no sabemos quién ni cómo, pero continúa en funcionamiento.

IV.b.4 Los errores confirmados del SRF.

El propio Ministerio nos brinda datos que nos dejan a la clara del mal desempeño y la falta de entrenamiento que tiene el sistema de identificación de prófugos o sistema de identificación biométrico cuando se nos plantea que 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 qué porcentaje representa del total de alertas arrojadas (3059). Para ello, una regla de tres simple será suficiente:

1648/3059=0.538738*100= **53.87%** de efectividad.

Esto es muchísimo más bajo e impresentable de los fallos y falencias de un sistema informático que se encuentra en funcionamiento, prejuzgando a ciudadanos en la vía pública y sin el menor respeto por los DDHH de la ciudadanía en su conjunto y mucho menos respetando los tratados internacionales firmados por nuestro País sobre protección de datos personales.

IV.b.5 La existencia de una práctica discriminatoria contra las mujeres y minorías raciales residentes en la CABA.

Tanto el relator de la ONU como los periodistas con idoneidad relevan riesgos en términos de discriminación tanto en los casos internacionales como en el sistema usado en la Ciudad Autónoma de Buenos Aires: *"Diversos estudios confirman que el reconocimiento facial puede tornarse una tecnología que ayuda a amplificar los prejuicios de las fuerzas de seguridad si su implementación no es cuidadosa ni constante la evaluación y corrección de esos prejuicios. Sin embargo, el uso de métodos criptográficos deprecados desde hace mas de 20 años y la calidad gran mayoría de los sistemas comerciales estudiados en* http://proceedings.mlr.press/v81/buolamwini18a.html *permiten asumir que esos sistemas ponen en jaque el ejercicio de derechos fundamentales y garantías constitucionales, reforzando la discriminación según la tez o el género de las*

personas, además de poner en riesgo la presunción de inocencia y el debido proceso. En Estados Unidos, un análisis de los algoritmos de reconocimiento facial evaluados por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) encontró que el desempeño del software es más preciso cuando se usa sobre la población que lo desarrolló, lo que lleva a una discriminación en base a la tez o el género de las personas. Esto es particularmente preocupante dado que el tratamiento de esta tecnología se desarrolla mayormente por jóvenes, adultos, varones y blancos, pero luego se utiliza, principalmente, contra grupos vulnerables y minorías. Según la American Civil Liberties Union (ACLU), el reconocimiento facial falla en analizar con precisión a las personas con tez oscura, clasificando erróneamente a mujeres afroamericanas como hombres y evaluando a hombres afroamericanos como "agresivos" aunque su expresión facial sea neutral."Fuente la Nación. Natalia Zuazo.

El observatorio de derechos humanos, el relator realizó una declaración sobre el derecho a la privacidad y en cuanto al reconocimiento facial llevada adelante por la Ciudad Autónoma de Buenos Aires manifiesta los siguientes puntos:

19-" ...Los ejemplos de otras ciudades han demostrado que la mejora de la seguridad pública mediante la instalación de cámaras de vigilancia es cuestionable en algunos casos y justificable en otros. La justificación de tal sistema, su legitimidad, necesidad y proporcionalidad deberían haberse establecido mediante una evaluación del impacto en la privacidad (en inglés Privacy Impact Assessment, PIA) que no parece haberse llevado a cabo"

20" ...Soy consciente de la necesidad de detener a las personas sospechosas de haber cometido delitos y llevarlas ante la justicia, pero no veo la proporcionalidad de instalar una tecnología con graves implicaciones para la privacidad para buscar en una lista de 46.000 personas que actualice y compruebe cuidadosamente su exactitud."

23 "Me preocupa que ni Buenos Aires ni Comodoro Rivadavia hayan realizado ninguna evaluación de impacto en la privacidad antes de implementar amplias redes de cámaras de vigilancia o sistemas de reconocimiento facial y reconocimiento de matrículas. Los funcionarios y funcionarias a los que entrevisté dijeron que estaban seguros de que el derecho a la privacidad no estaba siendo violado por los sistemas existentes y que cumplían los requisitos legales, pero que no podían explicar su necesidad y proporcionalidad. En estos y otros casos similares es esencial que las evaluaciones preliminares de impacto se lleven a cabo inmediatamente y sin demora y que sus recomendaciones sobre salvaguardias y recursos se cumplan de inmediato."

Es deber entonces de V.S realizar el debido control de constitucionalidad y de convencionalidad de dicha normativa, la jurisprudencia ha dicho al respecto: *Es un contrasentido aceptar que la Constitución Nacional confiere rango constitucional a la Convención Americana sobre Derechos Humanos (art. 75, inc. 22), incorpora sus disposiciones al derecho interno y, por consiguiente, habilita la aplicación de la regla interpretativa -formulada por la Corte Interamericana de Derechos Humanos- que obliga a los tribunales nacionales a ejercer de oficio el control de convencionalidad y que ,por otro lado, impida a esos mismos tribunales ejercer similar examen con el fin de salvaguardar su supremacía frente a normas locales de menor rang*o. Fallos: 335:2333

Por lo expuesto solicitamos que se de a lugar a esta acción de amparo en todas sus partes, con costas a cargo del demandado.

V.- FUNDAMENTOS DE DERECHO.

V.a. Noción de Amenaza, Fallo Pisoni, Fallo Baeza, Doctrina.

Como podemos advertir la conducta dañosa recae en un marco potencial y ésto debe ser considerado como suficiente concreción e inmediatez, más aún cuando ya se ha implementado y sancionado normativa a tales fines, muestra de ellos es que el Gobierno de la Ciudad de Buenos Aires ya incurrió en la misma conducta de vulnerar distintos Derechos aquí mencionados y la propia Justicia de la Ciudad Autónoma de Buenos Aires en la fallo Pisoni Carlos Contra GCBA sobre Amparo Expte Nº 36689/10 ya ha resuelto que:

"...La Corte Interamericana de Derechos Humanos en el "Caso Almonacid Arellano y otros vs. Chile", sentencia del 26 de septiembre de 2006, Serie C No 154, párr. 124 ha expresado que "Cuando un Estado ha ratificado un tratado internacional como la Convención Americana, sus jueces, como parte del aparato del Estado, también están sometidos a ella, lo que les obliga a velar porque los efectos de las disposiciones de la Convención no se vean mermadas por la aplicación de leyes contrarias a su objeto y fin y que desde un inicio carecen de efectos jurídicos. En otras palabras, el Poder Judicial debe ejercer una especie de "control de convencionalidad" entre las normas jurídicas internas que aplican en los casos concretos y la Convención Americana sobre Derechos Humanos. En esta tarea, el Poder Judicial debe tener en cuenta no solamente el tratado, sino también la interpretación

que del mismo ha hecho la Corte Interamericana, intérprete última de la Convención Americana".

En este marco, se han detallado los informes emitidos por el Comité contra la Tortura de la ONU, quien ha sido explícito y contundente en cuanto a que las armas Taser X 26 constituyen una forma de tortura que los Estados Parte deben impedir.

No debe olvidarse que este Comité es un órgano esencial de la Convención, y que su función es cooperar con los Estados Parte para que garanticen el ejercicio y goce de los derechos, de modo que adopten las medidas legislativas y administrativas necesarias para ello.

Así, el artículo 20 de la mentada Convención señala que si el Comité recibe información fiable que parezca indicar que en un Estado se practica sistemáticamente la tortura, éste órgano lo invitará a cooperar en el examen de la información y a presentar observaciones al respecto, pudiendo el Comité designar a uno o varios de sus miembros para que procedan a una información confidencial que puede incluir una visita a su territorio.

De este modo, y en torno a la manera en que el Comité se expide, Mónica Pinto ha señalado que: "El diseño está esencialmente basado en el método del diálogo, esto es, que se persigue una suerte de 'conversación' entre el Estado y el órgano de control que permita cumplir con el objetivo de conocer hasta dónde se garantizan los derechos protegidos" (Pinto, Mónica, Temas de Derechos Humanos, Editores del Puerto, Buenos Aires, 1998, pág. 126).

De allí que las recomendaciones aún efectuadas en tono potencial por parte del Comité, deban ser vistas igualmente con la fuerza vinculante necesaria como para obligar a los Estados suscriptores del Tratado, además de tener una finalidad preventiva. De otro modo, no se entendería a qué fines un Estado decide asumir un compromiso internacional.

Agrega la autora: "Probablemente, lo más valioso del sistema de informes sea su capacidad de actuar como un elemento de prevención. En efecto, el conocimiento de las situaciones que obstaculizan el pleno goce y ejercicio de los derechos humanos en un determinado contexto nacional permite definir políticas para superarlas que, con sus más o sus menos, actúan como un elemento de prevención" (Pinto, Mónica, op. cit., pág. 128/129).

Reconocer la dignidad de las personas a la luz de los tratados internacionales que el Estado Argentino ha decidido suscribir implica indefectiblemente aceptar que el Estado no puede proferir tratos crueles, inhumanos o degradantes que provoquen sufrimientos o dolores intensos, tal como lo ha descripto el Comité contra la Tortura. Si esta es la calificación que

ese Comité ha efectuado de las armas Taser, debe estarse a esas conclusiones, y admitir que hemos decidido vivir en una sociedad donde deseamos que ciertos hechos no sucedan "NUNCA MAS...".

Como podemos advertir en el Fallo emitido por La Jueza Andrea Danas que el mismo cuenta con algunos argumentos similares en cuanto a la potencia del bien jurídico afectado y el control de convencional y constitucional aquí planteado, como se puede observar los derechos colectivos homogéneos afectados y el interés simple aquí manifestado concuerdan no solo con lo establecido en el Fallo Halabí sino por el cual la Jueza dio lugar al fallo aquí vertido.

En el Fallo Baeza C/ Estado Nacional 306:1125 sentido, la Corte Suprema de Justicia ha señalado que "la necesidad de la existencia de 'caso' o 'controversia' como premisa para el ejercicio del Poder Judicial", supone la existencia de "pautas que permitan establecer si se da una controversia definida y concreta...(mencionando entre ellas) las siguientes: a) que la acción (administrativa) impugnada afecta sustancialmente en algún momento los intereses legales de alguna persona; b) que la actividad cuestionada afecta al peticionante en forma suficientemente directa; y c) que ella ha llegado a una concreción bastante en el ámbito administrativo (...) la necesidad de que el interés invocado tenga suficiente inmediatez y realidad también en los supuestos de acciones de mera certeza".

Así mismo y a la luz de ambos fallos (Pisoni, Baeza) el Doctor Juan Ignacio Sáenz en su obra " Legitimación del Ciudadano, el elector, el contribuyente. La legalidad objetiva como bien colectivo" nos ilumina de la siguiente forma "La historia del control de oficio en nuestro país es por demás conocida, así como lo son los argumentos en que se apoyan las posiciones a favor y en contra. Sólo me interesa destacar que la facultad de pronunciar una inconstitucionalidad de oficio ha sido recibida definitivamente en el caso Banco Comercial de Finanzas (2001), en los siguientes términos: "[S]i bien es exacto que los tribunales judiciales no pueden efectuar declaraciones de inconstitucionalidad de las leyes en abstracto, es decir, fuera de una causa concreta en la cual deba o pueda efectuarse la aplicación de las normas supuestamente en pugna con la Constitución, no se sigue de ello la necesidad de petición expresa de la parte interesada, pues como el control de constitucionalidad versa sobre una cuestión de derecho y no de hecho, la potestad de los jueces de suplir el derecho que las partes no invocan o invocan erradamente trasuntado en el antiguo adagio iura novit curia incluye el deber de mantener la supremacía de la Constitución (art. 31 de la Carta Magna) aplicando, en caso de colisión de normas, la de mayor rango." Lo interesante además es que se descartó que el control de oficio comprometiera el equilibrio de poderes en favor del judicial y en mengua de los otros dos,

tal como históricamente se había sostenido, pues carece de consistencia lógica sostener que existe un indebido avance sobre los otros poderes por el sólo hecho de no haber mediado petición de inconstitucionalidad por una de las partes, y que en cambio esa invasión se tiene por no operada si medió tal planteo en el proceso.

Efectos generales de las sentencias: Está claro que no existe en nuestro país —en el ámbito federal— el efecto derogatorio de las sentencias, y que ese mecanismo sólo sería posible por vía de una reforma constitucional que establezca semejante efecto jurídico "de pleno derecho" y de modo automático. Sin embargo, a mi entender es posible apreciar ciertos "efectos generales no derogatorios" en muchos pronunciamientos y sentencias de la Corte Suprema, lo cual quiere decir, sencillamente, que están dirigidas a una pluralidad de sujetos indeterminados —a la sociedad y a los demás poderes del Estado— y que por ende no existe en rigor un efecto acotado a quienes han sido parte en la causa en su sentido tradicional. Los mencionados efectos generales se ha dado por tres vías o modalidades distintas: a) Por el efecto erga omnes expresamente otorgado a una sentencia, como el caso Halabi que comento adelante, y b) por el dictado de exhortaciones dirigidas al Congreso de la Nación, al Poder Ejecutivo Nacional o a Estados locales, tal como ha ocurrido en algunos precedentes y tiende a ocurrir cada vez más. El tan temido efecto erga omnes de las sentencias ya cuenta con un cuerpo importante de precedentes, pero por lo novedoso sólo me voy a referir a los recientes casos Rosza (2007) y Halabi (2009)"

En Halabi, la Corte declaró la inconstitucionalidad de la ley 25.873, en cuanto autorizaba la intervención de las comunicaciones telefónicas sin precisar debida-mente los fundamentos ni regular la intervención judicial necesaria para habilitar las intromisiones a la privacidad y a la intimidad garantizadas en los arts. 18 y 19 de la Constitución nacional. Consideró que el actor —Ernesto Halabi— era titular de un derecho de incidencia colectiva referente a intereses individuales homogéneos, por lo que la sentencia debía extenderse a todo el resto de usuarios del servicio de telecomunicaciones. En el caso Arriola (2009), además de declarar la inconstitucionalidad de la penalización de la tenencia de estupefacientes para consumo personal, finalizó el pronunciamiento de la siguiente manera: "Exhortar a todos los poderes públicos a asegurar una política de Estado contra el tráfico ilícito de estupefacientes y a adoptar medidas de salud preventivas, con información y educación disuasiva del consumo, enfocada sobre todo en los grupos más vulnerables, especialmente los menores, a fin de dar adecuado cumplimiento con los tratados internacionales de derechos humanos suscriptos por el país. Por último, es importante que señale que si bien el concepto de caso judiciales de aquellos de carácter indeterminado, y su concepción no sólo varía en los diferentes ordenamientos en que se aplica, sino que además se ha visto modificado con los años en nuestro orden federal, aun así cabe

reconocerle cierto marco mínimo determinado por los siguientes elementos: a) Que el sujeto actor plantee un conflicto de derecho con suficiente seriedad de fundamentación y precisión acerca de aquello que peticiona y del interés que considera afectado; b) que dicho conflicto sea actual y no abstracto, remoto, prematuro o hipotético, y c) que la cuestión constitucional se encuentra planteada, como ha dicho la Corte muchas veces, con la claridad y el esfuerzo de argumentación que la inteligencia de la Constitución exige".

Como vemos el análisis realizado por el Doctrinario Sáenz es contundente y actual al análisis que venimos invocando.

La extracción del texto corresponde al Sitio web del Dr Gordillo. https://www.gordillo.com/pdf_unamirada/04saenz.pdf

V.b Derechos Conculcados.

V.b.I Derecho de Reunión.

El reconocimiento facial atenta contra el derecho de reunión, dado que varios estudios indican que las personas actúan con temor cuando saben que están siendo vigiladas, por lo que procurarás dejar de reunirte o alejarte de ese espacio de vigilancia.

Al derecho de reunión no debe ejercerse control de su ejercicio, el mismo es de vital importancia para una democracia, y el mismo no puede ser limitado ni restringido.

Como los descripto en el artículo 5 de la ley Nº 6.339 que modifica el artículo 484 de la ley Nº 5.688 que establece que el SRP recolecta información aún sin orden judicial solamente con la mera "investigación Policial" ya es suficiente para que las imágenes, videos y toda información biométrica de la ciudadanía (aún la de personas extranjeras, menores de edad, militantes políticos, etc) quede en manos de una Fuerza sin el deber de destrucción y la falta de obligatoriedad. Y el acto administrativo de la Resolución N° 398/MJYSGC/19 que puso en funcionamiento el sistema de reconocimiento de prófugos. El derecho a reunión se ve afectado en su máxima plenitud cuando existiendo riesgos con mencionadas minorías (color, raza, religión, políticas) son objeto de errores en las detecciones por parte de un sistema automatizado como ocurre en Países como Estados Unidos donde dejaron de utilizar sistemas de reconocimiento facial (biométricos) por la gran afectación a los derechos civiles y políticos de las minorías. En nuestro País ese mismo problema existe en cuanto a minorías ante reclamos políticos y sociales, además de religiosos, raza, color,

salud y también en respeto por los derechos políticos y civiles de cada uno de los ciudadanos que transita por la Ciudad Autónoma de Buenos Aires, con el derecho a hacerlo y sin el juzgamiento de un sistema informático que lo restrinja.

V.b.II Protección de Datos Personales y Tratados Internacionales.

En la ley de protección de datos personales, Ley Nº 25.326, los datos biométricos son considerados de los datos más sensibles que cualquier persona puede tener, es decir uno no puede cambiar sus rasgos físicos, su caminar, su accionar normal y habitual, con los que nos lleva a tener un agente de tratamiento de datos personales sensibles, sin un responsable y todas las indicaciones emitidas por la Dirección Nacional de Protección de Datos Personales como la resolución 4/2019 anexo I Criterio 4 segundo párrafo "... Los datos biométricos que identifican a una persona se considerarán datos sensibles (conforme el artículo 2°, Ley N° 25.326) únicamente cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su titular (v.g. datos que revelen origen étnico o información referente a la salud)..." Lógicamente en el reconocimiento facial no ha sido considerado un informe de impacto como es lo solicitado en el Convenio 108 del cual Argentina es Estado parte y es una de las condiciones aceptadas para ser "País Seguro" ante la Unión Europea por cuestiones de Datos Personales, donde cada una de las Autoridades de Control (en el caso Nacional son la Dirección Nacional de Protección de Datos Personales y la Agencia de Acceso a la Información en caso de la Ciudad Autónoma de Buenos Aires es la Defensoría del Pueblo, donde no hay informe o comunicación emitida sobre dicho informe) deben realizarlo y además es un convenio firmado con el País vecino, Uruguay (incluso hasta la guía propuesta para cumplir con dicho informe fue realizada por las autoridades de aplicación de Argentina y Uruguay), aprobado por Ley Nº 27.483 y han seguido las más modernas legislaciones y guías en la materia, con particular atención a los Estados miembro de la Unión Europea y a los Estados parte del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personales -tratado internacional que tanto Argentina como Uruguay han suscrito y ratificado - donde estamos obligados a cumplir. Motivo por el cual ninguno de los artículos se refiere a la necesidad de cumplir con los tratados internacionales en cuanto a la necesidad de un informe de impacto y ello no puede quedar sujeto a una posterior reglamentación por parte de la autoridad de control dado que en el marco de la ley no se encuentra sancionado y como principio básico " lo que no se encuentra prohibido, está

permitido” hace que la normativa sea contraria la normativa nacional y a los diferentes Convenios y Tratados internacionales.

Así mismo, la Ciudad Autónoma de Buenos Aires posee la Ley Nº 1845 del año 2005 que versa sobre Protección de Datos Personales, cuyo órgano de control es la Defensoría del Pueblo, donde se protege entre otras cosas la Transferencia Inter Provincial e Internacional de datos sensibles (Art. 12) que lógicamente deberían ser cumplidos pero no sabemos cual es cumplimiento dado que no se encuentra un informe previo de impacto y tampoco la estructura propia de hardware sobre la que funciona el SRF.

En los fundamentos del acto administrativo de la Resolución 398/MJYSGC/19 indican “...Que la utilización del sistema integral de video vigilancia está regida por el principio de proporcionalidad y razonabilidad, en su doble versión de procedencia y de intervención mínima. La procedencia determina que sólo podrá emplearse cuando resulte adecuado, en una situación concreta, para asegurar la convivencia ciudadana, la utilización pacífica de las vías y espacios públicos, la elaboración de políticas públicas de planificación urbana, así como para la prevención de faltas, contravenciones y delitos y otras infracciones relacionadas con la seguridad pública;Que la intervención mínima exige la ponderación en cada caso de la finalidad pretendida y la posible afectación al derecho a la propia imagen, a la intimidad y a la privacidad de las personas, de conformidad con los principios consagrados en la Constitución Nacional y la Constitución de la Ciudad Autónoma de Buenos Aires;Que la Ley Nacional Nº 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…” Los principios de proporcionalidad y razonabilidad vemos que no son cumplidos pero sí reconocidos por el Acto administrativo dado que no toma en cuenta lo vertido por las normas Nacionales y los Tratados Internacionales, cabe destacar que el artículo 5 de la Ley Nº 25.326 sobre Consentimiento, el legislador la tomó desde la Ley Española que dicho artículo ha sido declarado Inconstitucional fallo STC 2992/2000 donde el Tribunal Constitucional español detalla:

“ Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros (...) Dicha peculiaridad radica en su contenido, ya que (...), el derecho a la protección de datos atribuye a su titular un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos (..), y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos

personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales"(F.J. 6, cuarto párrafo). El fundamento jurídico 7 de la referida sentencia viene a remarcar el contenido del derecho fundamental a la protección de datos y las facultades que proporciona al individuo tanto frente al Estado como ante el particular. Dice el citado fundamento jurídico: " De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede éste tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida , la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no , de los datos personales requiere como complementos indispensables , por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y , por otro lado, el poder oponerse a esa posesión y usos…" como bien cita el trabajo doctrinario del Magistrado Juan Manuel Fernández López (ex director de la Agencia de Protección de datos de España) en su obra titulada "El Derecho Fundamental a la Protección de Datos Personales. Obligaciones que Derivan para el Personal Sanitario", cuyo enlace se agrega en la Prueba Documental. Como observamos la Interpretación que realiza el Gobierno de la Ciudad de Buenos Aires sobre el Artículo 5 de la Ley Nº 25.326 es erróneo y no cumple con ningún estándar de razonabilidad o proporcionalidad.

V.b.II.a Política Modelo de Seguridad de la Información.

Como es lógico, nuestro País tiene un "modelo" sobre los distintos análisis a llevar adelante en cuanto a la seguridad que deben tener los sistemas que manejan información o datos sensibles, entendamos que los datos biométricos son aquellos más sensibles dado que además de denostar una imagen, también dan orígenes a Raza, Color, Etnia, Religión, Condición Política, Salud, y por ello es que se deben cumplir con los más altos mecanismos de seguridad, esto fue regulado mediante las Disposición 1/2015 de la Oficina Nacional de Tecnologías de la Información (ONTI) donde dan un sinfín de requisitos y

análisis, casualmente no difieren en el espíritu del deber de cuidado de la resolución 47/2018 de la Agencia de Acceso a la Información Pública en relación a velar por la seguridad de los datos (o información) que debe ser de forma previa a la implementación de un sistema como el de Reconocimiento Facial de Prófugos, mediante los datos más sensibles que una persona pueda tener, y su correspondiente relación para el total de ciudadanos que pasan por debajo de una de las cámaras de éste sistema que como queda claro: no tiene capacidad para NO tomar los datos de terceras personas, por el contrario, lo hace para que su IA (Inteligencia Artificial) aprenda, realizando tratamiento de datos personales de los más sensibles que hay al momento. Entonces lo expuesto por el artículo 6 de la Ley Nº 6.339 que modifica el artículo 490 de la Ley Nº 5.688 obliga a la Autoridad de Control a crear un registro en el que figuren "todos los registros" solamente explicando su "estado operativo" es decir si se encuentra funcionado, qué software y hardware se utilizan pero no solo el plazo de un año es considerablemente escaso sino que no cumple con las distintas pautas solicitadas en cuanto a seguridad de la información.

V.b.IV.d. Ausencia de controles en la política de permisos - Derecho a la Intimidad.

Como es notorio y de público conocimiento, en la Causa Super Mario Bross, que versa sobre el espionaje ilegal y sistemático realizado por el grupo de la Agencia Federal de Inteligencia donde la Política de Seguridad de Centro de Monitoreo Urbano (CMU), en cuanto a su Política de Permisos se vió afectada dado que en dicho expediente figuran un gran número de imágenes y vídeos de dicho organismo, con lo cual nos hace plantear una falta de razonabilidad sobre quienes manejan el SRF y las falacias en cuanto a controles establecidos por los mismos. El riesgo a perder el control de los datos biométricos de los ciudadanos es carente de proporcionalidad ante el bien jurídico que se intenta esgrimir existiendo alternativas válidas para la detección de prófugos sin tener consecuencias para el total de la población y con un error de identificación del %57 (aprox) sobre el total de personas "demoradas". Sin tener en cuenta que el Jefe de Gobierno de CABA habría cedido las imágenes obtenidas por las Cámaras del CMU a la AFI para que un periodista sepa quien pegó unos carteles en la vía pública, una falta de proporcionalidad manifiesta.

En la normativa aquí cuestionada no hay un control suficiente sobre los Registros y hasta da cuenta que el Poder Ejecutivo y las Fuerzas Policiales tienen acceso a la Información Biométrica obtenida de todas las personas que sean tomados por las distintas Cámaras, como explicamos el SRF tiene una Inteligencia Artificial que para aprender genera una base de datos de la totalidad de las personas y cuando compara con cierto patrón alguna

información que provenga de la base de CONARC lanza el alerta (con un %57 de error) pero ya prejuzgo, almacenó y recabó información biométrica de la totalidad de las personas, ésto no se encuentra reglado por los artículos creados por la Ley Nº 5.339 al agregar el artículo 480 bis a la Ley Nº 5.688 sino que al prohibirlo en forma deficiente hace que el sistema recaiga en errores y sea de implementación imposible por la forma en que funcionan los sistemas en tiempo real.

V.b.IV.a. Derecho a la no discriminación.

En los procesos civiles relativos a la ley 23.592, en los que se controvierte la existencia de un motivo discriminatorio en el acto en juego, 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 tuvo como causa un motivo objetivo y razonable ajeno a toda discriminación, y la evaluación de uno y otro extremo, es cometido propio de los jueces de la causa, a ser cumplido de conformidad con las reglas de la sana crítica.(334:1387)

La ley antidiscriminatoria es una regla general que vino a ampliar la cobertura que, ante una misma situación, prevén las leyes especiales, sin que de su letra surja restricción alguna de la que pueda derivarse incompatibilidad con las normas que contemplan un resarcimiento económico ni la exclusión de un colectivo de personas del remedio que el legislador quiso como regla (341:1106).

En el marco que plantea la Constitución de 1994, la igualdad debe ser entendida no solo desde el punto de vista del principio de no discriminación, sino también desde una perspectiva estructural que tiene en cuenta al individuo en tanto integrante de un grupo, considerando el contexto social en el que se aplican las disposiciones, las políticas públicas y las prácticas que de ellas se derivan, y de qué modo impactan en los grupos desventajados, si es que efectivamente lo hacen. Todo lo cual conlleva la utilización de criterios de control de constitucionalidad más estrictos que aquel generalmente utilizado para evaluar los casos desde el enfoque tradicional de la igualdad.(340:1795)Para decidir si una diferencia de trato es ilegítima se analiza su mera razonabilidad; esto es, si la distinción persigue fines legítimos y constituye un medio adecuado para alcanzar esos

fines. Sin embargo, cuando las diferencias de trato que surgen de las normas están basadas en categorías "específicamente prohibidas" o "sospechosas" corresponde aplicar un examen más riguroso, que parte de una presunción de invalidez. En estos casos, se invierte la carga de la prueba y es el demandado quien tiene que probar que la diferencia de trato se encuentra justificada por ser el medio menos restrictivo para cumplir un fin sustancial (doctrina de Fallos: 327:3677; 332:433, considerando 6° y sus citas).(340:1795)

Los sistemas de reconocimiento facial (SRF) funcionan mediante la comparación de características biométricas de dos rostros. Para poder llevar a cabo esta tarea, deben aprender cuándo se trata de la misma persona y cuándo no. Esto lo logran a partir de una base de datos de distintas caras.

Sin embargo, dado que estas bases de datos tienen predominancia de hombres blancos cisgénero, los SRF aprenden mejor cómo diferenciar a dos personas con estas características que al resto de la población. El resultado es que la mayoría de estos programas presentan sesgos.

Es notorio que los SRF están siendo juzgados por discriminación y dejados de lado por el mismo motivo, en los Estados Unidos ciudades como Massachussetts ya a suspendido (ví judicial) la aplicación de Sistema de Reconocimiento Facial (como el aquí cuestionado) por poseer un gran sesgo en cuanto a discriminación por RAZA, COLOR Y ETNIA, recordemos que una de las Universidades más importantes en cuanto al desarrollo de tecnología se encuentra en ese mismo lugar, hablamos del MIT.

Existen distintos estudios que verifican estos inconvenientes, incluso en software de grandes empresas como Amazon, IBM y Microsoft: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Frente a esta situación, se elevó un pedido de acceso a la información pública. El Gobierno de la Ciudad de Buenos Aires respondió que “se realizaron pruebas sobre una población controlada de personas seleccionadas dentro del equipo de trabajo (personal de la Policía de la Ciudad y del Ministerio de Justicia y Seguridad). Se consideraron personas con características físicas disímiles y con diferentes accesorios que impedían ver completamente sus rostros (tales como anteojos, gorros, capuchas, barba, bigotes, etc.). Asimismo, los test involucraron distinto tipo de cámaras, ángulo, iluminación y ambientes (aire libre, bajo superficie, de día y de noche).” (NO-2019-23068285-GCABA-DGEYTI).

Esta respuesta da a entender que se comprende la gravedad del problema planteado. Sin embargo, no se ofrecen detalles sobre los resultados más allá de sostener que las pruebas fueron satisfactorias, lo que vuelve imposible una mayor rigurosidad en el análisis. Sería deseable conocer la eficacia del SRF según distintas características como género, edad, etnia, nacionalidad.

En respuesta a otro pedido de acceso a la información pública (NO-2019-33745359-GCABA-DGEYTI) no se logró tampoco obtener acceso al código fuente del sistema, ni al conjunto de datos ("dataset") utilizado para su entrenamiento. Nuevamente esto no permite a la sociedad realizar su propia evaluación del sistema.

Pero por sobretodo, genera un conflicto enorme para personas que son Mellizas, Gemelas, y algo que es aún más complejo personas que tienen rostros con rasgos "comunes" y estos sistemas no están contemplados para que distingan sino para que comparen.

V.X.- EL ESCRUTINIO ESTRICTO EN CASOS DE DISCRIMINACIÓN – SU APLICABILIDAD AL CASO.

V.X.- La ausencia de auditoría de los datasets empleados como óbice insuperable para la detección de sesgos discriminatorios en el funcionamiento del sistema.

V.X.- Antecedentes en jurisdicciones comparadas.

V.X. San Francisco

La existencia de estos sesgos ya ha llevado a la prohibición de su implementación en distintas ciudades. En San Francisco, por ejemplo, el considerando (d) dice "La propensión de la tecnología de reconocimiento facial a poner en peligro los derechos civiles y las libertades civiles supera sustancialmente sus supuestos beneficios, y la tecnología exacerbará la injusticia racial y amenazará nuestra capacidad de vivir sin la supervisión continua del gobierno." (https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019).

V.X. Massachusetts

La ciudad de Boston ya prohibió el uso de reconocimiento facial (https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban) y también se está tratando un proyecto para la prohibición de SRF en el estado bajo el argumento de que "muchas de las bases de datos a las que se aplica la tecnología de reconocimiento facial están plagadas de disparidades raciales y otros sesgos, que generan sesgos de imitación en los datos de reconocimiento facial." (https://malegislature.gov/Bills/191/S1385).

V.X. Europa

Los SRF también han recibido fallos en su contra por estos motivos en el Reino Unido (https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/).

En La sentencia del Caso Nº C1/2019/2670 con sentencia de fecha 11 de agosto de 2020 se tomó el Sistema de Reconocimiento Facial y la Corte señalo que el sistema de Reconocimiento Facial Biométrico es desproporcional en cuanto al riesgo tomado en función del valor jurídico protegido (Considerando 44). En cuanto al tratamiento de datos personales es tajante (Considerando 46) "...El principal punto de disputa ante el Tribunal Divisional en virtud de la DPA de 1998 fue el hasta qué punto el uso de AFR Locate implica el procesamiento de datos personales, SWP sostiene que los únicos datos personales procesados son los datos de las personas en la lista de observación en el sobre la base de que son solo esas personas a las que SWP puede identificar por su nombre. Habiendo referido a la sentencia del Tribunal de Apelación en Vidal-Hall v Google Inc [2015] EWCA Civ311, [2016] QB 1003, y a la decisión del TJUE en el asunto C-212/13 Rynes / Urad[2015] 1 WLR 2607, el Tribunal Divisional concluyó (en [122]) que la tramitación de la imagen del apelante por el equipo AFR Locate estaba procesando sus datos personales porque la información registrada por AFR Locate lo individualizó de todos los demás, que es decir que lo destacó y distinguió de todos los demás.

En los Considerandos 64, 65 y 66 El Estado, quien resulta apelante, intenta hacer creer que es un sistema de investigación abierto y que la comparación de datos biométricos es similar a lo realizado con huellas dactilares, ésto es refutado de pleno y las comparaciones dejadas de lado, donde no pudo demostrarse que las injerencias sobre la sociedad en su conjunto son necesarias. Aún los registros de ADN son menos riesgosos que el tratamiento de datos biometricos de toda la población indica la Corte. La Sentencia es notoria: "...El uso por parte del Demandado de la tecnología de reconocimiento facial automatizado en vivo en 21 Diciembre de 2017 y 27 de marzo de 2018 y de forma continua, que comprometió el

artículo 8 (1) del Convenio Europeo de Derechos Humanos… El uso continuo por parte del Respondedor de la tecnología de reconocimiento facial automatizado en vivo, sus datos. La Evaluación de Impacto de Protección no cumplió con la sección 64 (3) (b) y (c) de los Datos Ley de Protección 2018.La Demandada no cumplió con el Deber de Igualdad del Sector Público en la sección 149 de la Ley de Igualdad de 2010 antes o en el curso de su uso de Tratamiento facial automatizado en vivo Tecnología de reconocimiento el 21 de diciembre de 2017 y el 27 de marzo de 2018…"

V.X Suecia - Municipio de Skelleftea.

Multa de 20 000 USD por violación a la GDPR

https://www.compliancejunction.com/unlawful-use-of-facial-recognition-technology-lead-to-gdpr-penalty-in-sweden/ Conforme surge de èste articulo: "La Autoridad Sueca de Protección de Datos (DPA) ha multado al municipio de Skelleftea con 200,000 coronas suecas (£ 16,800, $ 20,700) por violar la ley general de protección de datos de la Unión Europea (GDPR) al probar el reconocimiento facial en estudiantes de secundaria en Suecia para realizar un seguimiento de la asistencia .

La escuela en el centro de la violación de GDPR afirmó, durante la investigación del incidente, que el proceso fue consensuado. Sin embargo, la DPA sueca argumentó que un acuerdo consensuado no podría tener una base legal válida debido al desequilibrio de poder entre el interesado y el responsable del tratamiento.

La prueba de tecnología de reconocimiento facial se estaba llevando a cabo, con la empresa de TI Tieto, para monitorear la asistencia de los estudiantes durante tres semanas hacia fines de 2018. La prueba incluyó el uso de cámaras de seguridad y tecnología de reconocimiento facial para monitorear la asistencia de 22 estudiantes a la escuela. . La escuela esperaba determinar si la tecnología de reconocimiento facial podría usarse en lugar de pasar lista estándar en las clases. Se esperaba que el uso de la tecnología anularía el requisito, en virtud de la legislación sueca, de que las escuelas pasen lista al comienzo de cada lección. Este deber puede afectar la cantidad de tiempo de enseñanza real durante cada período de clase. La escuela afirmó que estaba perdiendo 17.280 horas al año simplemente marcando la asistencia. T

La DPA determinó que la escuela violó varios artículos del GDPR, a pesar de tener las mejores intenciones al realizar el juicio. Declaró que la escuela procesó ilegalmente los datos biométricos de sus estudiantes y no realizó una evaluación de impacto adecuada ni notificó a la DPA sobre el piloto. Los datos de reconocimiento facial se tratan como información confidencial y requieren una mayor protección que otros tipos de datos menos sensibles.

Los representantes de la escuela en la audiencia afirmaron que había obtenido el consentimiento de todos los estudiantes involucrados en el piloto. Sin embargo, la DPA determinó que el consentimiento no era válido porque había "un claro desequilibrio entre el interesado [estudiante] y el controlador [municipio]".

El RGPD se introdujo el 25 de mayo de 2018, después de un período de dos años, para salvaguardar la privacidad de los ciudadanos de la UE y darles más poder en relación con el uso de sus datos personales. La sanción financiera podría haber sido de hasta 1 millón de euros (1,1 millones de dólares) por las infracciones del RGPD".

V.X Russia – Moscú.

El siguiente articulo informa: https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged "La activista Alyona Popova y el político Vladimir Milov presentaron una denuncia por el uso de tecnología de reconocimiento facial por parte de Rusia durante las protestas ante el Tribunal Europeo de Derechos Humanos.

Su abogado, Kirill Koroteyev, dijo que este sería el primer caso que impugna el uso de la tecnología de reconocimiento facial para llevar a cabo una vigilancia masiva en la práctica del tribunal.

El 29 de septiembre de 2019, al menos 20.000 personas, incluidos Popova y Milov, participaron en un mitin autorizado en Moscú en solidaridad con los detenidos y acusados por su participación en protestas pacíficas. Las manifestaciones fueron provocadas por la exclusión de candidatos independientes de las elecciones legislativas de la ciudad de Moscú.

Según Popova y Milov, todos los participantes de la protesta de septiembre tuvieron que pasar por detectores de metales equipados con cámaras CCTV instaladas a la altura de los ojos. El gobierno de Moscú anunció planes poco antes de las protestas para utilizar la tecnología de reconocimiento facial en grandes reuniones públicas. Los solicitantes creen que este fue el primer caso en que las autoridades de Moscú utilizaron tecnología de reconocimiento facial para recopilar datos sobre los manifestantes.

En enero, los solicitantes presentaron una denuncia interna contra el gobierno de Moscú. Koroteyev, jefe del programa de justicia internacional en Ágora, dijo que durante una audiencia judicial en enero en Moscú, un representante del Departamento de Tecnología de la Información de Moscú confirmó el uso de la tecnología de reconocimiento facial para realizar una vigilancia masiva en la protesta. En marzo, el tribunal desestimó la denuncia, alegando que el uso de la tecnología por parte del gobierno era legal.

La recopilación de datos biométricos únicos de los manifestantes mediante el uso de tecnología de reconocimiento facial viola el derecho a la privacidad y la libertad de reunión, tal como lo protege el Convenio Europeo de Derechos Humanos, argumentan Popova y Milov en su solicitud. También afirman que el uso de esta tecnología en un mitin de la oposición equivale a una discriminación basada en opiniones políticas.

La ley rusa requiere el consentimiento explícito para la recopilación gubernamental y privada de datos biométricos a través de la tecnología de reconocimiento facial, aunque hay excepciones establecidas en el conjunto de leyes vagas sobre seguridad pública y lucha contra la delincuencia.

El artículo 6 del Convenio para la protección de las personas en lo que respecta al procesamiento de datos personales (Convenio 108+), firmado por Rusia, subraya la importancia de las salvaguardias legales adecuadas para el procesamiento de los datos biométricos obtenidos mediante la tecnología de reconocimiento facial. Koroteyev señaló que estas salvaguardas faltan bajo la ley rusa, especialmente dada la ausencia de

supervisión judicial o pública sobre los métodos de vigilancia, incluido el reconocimiento facial.”

VI.- Daño Existente.

Para efectuar la detección de los prófugos en la vía pública, el sistema debe procesar las características faciales de cualquier transeúnte de la Ciudad para realizar la comparación, sin que él mismo haya dado su consentimiento, incluyendo información biométrica de menores.

Crecientemente los rasgos biométricos se usan como medidas de identificación y de seguridad de forma automatizada con el consentimiento informado de cada ciudadano. El sistema contratado no es de código fuente abierto (NO-2019-33745359-GCABA-DGEYTI) por lo que es imposible saber qué hace la empresa contratada con la información que obtiene, dando por plano lo normado en la ley Nº 6.339 al modificar el artículo 2 de la Ley Nº 5.688 dado que los tres sistemas (identificación, prevención, forense) requieren que cualquier persona sea “juzgada” por un sistema de Inteligencia Artificial sin la posibilidad de estar a derecho y solicitar consentimiento alguno a las personas, pero peor aún es que no contamos con la posibilidad que la Autoridad de Control pueda realizar auditorías en materia de datos personales (como el informe de impacto) o de seguridad informática (en cuanto a desarrollo de software y a seguridad en la conservación de bases de datos) porque solo se requiere especificaciones y una vez por año. Es decir que aún la cantidad de Copias Forenses no son determinadas, recordemos que una de las capacidades de las copias forenses es ser 100% iguales al original sin alterar el original, podemos tener infinidad de copias forenses sin la obligación de registro alguno con una mera investigación policial. La falta de consentimiento expreso degrada la privacidad de la sociedad en su conjunto.

Recordemos que el sistema de Reconocimiento Facial de Prófugos fue implementado mediante el acto administrativo de la Resolución N° 398/MJYSGC/19 donde aún no se estableció que datos utiliza el sistema informático ni cómo, porque rigen restricciones de Derechos de Autor en el proceso de Ley Nº 104.

Así mismo cabe recordar el deber de evitar un daño consagrado en el artículo 1710 del Código Civil y Comercial de la Nación Argentina que es de aplicación en todo el territorio por ser un Código de Fondo. Entendemos que las medidas aquí solicitadas hacen realmente uso de lo citado en dicho artículo 1710 dado que el Sistema de Reconocimiento Facial de

Prófugos aumenta el riesgo a niveles poco razonables en todo el mundo y nuestro derecho interno nos indica como un DEBER en cuanto de nosotros dependa.

Una investigación del Congreso de los Estados Unidos dice que “la capacidad de una plataforma para mantener redes sólidas mientras degrada la privacidad del usuario razonablemente puede considerarse equivalente a la decisión de un monopolista de aumentar los precios o reducir calidad del producto” (https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf). En ese caso el objeto de estudio son las prácticas monopólicas de empresas, pero la conclusión de que una pérdida de privacidad es equivalente a un daño para el ciudadano se mantiene.

VI.b. La configuración de una situación riesgosa.

Ningún sistema informático está completamente seguro ya que su mera existencia crea la posibilidad de que sea atacado, por más medidas de seguridad que se adopten.

Distintos organismos públicos han sido susceptibles de ataques exitosos con la peculiaridad de exigir dinero a cambio de no publicar datos. Recientemente ha ocurrido con la Dirección Nacional de Migraciones y el portal argentina.gob.ar, anteriormente con la Policía Federal.

La presencia de un sistema que realiza reconocimiento facial de personas en la vía pública, continuamente y en toda la ciudad origina inherentemente un nuevo riesgo para la ciudadanía: de ser accedido ilegítimamente la capacidad de daño es mayor que sin este sistema y, además, genera incentivos mayores para nuevas formas de extorsión.

Solo pensar la necesidad que tenemos en la obtención de una base de datos de todas las personas que visitan la Ciudad Autónoma de Buenos Aires (con los datos más sensibles que una persona pueda tener) y los distintos problemas de seguridad informática que surgen día a día en el planeta, además los mencionados de la propia Ciudad de Buenos Aires en causas Penales Federales, como la posible venta de la misma base por personal que una empresa privada que no sabemos a ciencia cierta que datos biométricos se encuentran “enseñando” a la Inteligencia Artificial es aceptar un riesgo desproporcionado en el bien a proteger, perdemos los datos biométricos de toda la población en “beneficio” tenemos una posibilidad de dar con una persona que se encontraría prófuga… con un %57 de error, por lo menos es irresponsable.

VII- Solicita dictado de medida cautelar de no innovar.

VII.a Verosimilitud en el Derecho.

Teniendo presente los derechos de raigambre constitucional en cuestión (derecho de trabajar, de informar y de otros derechos ya mencionados) la procedencia de las medidas cautelares, justificadas, en principio, en la necesidad de mantener la igualdad de las partes y evitar que se convierta en ilusoria la sentencia que ponga fin al pleito, queda subordinada a la verificación de los siguientes extremos insoslayables: la verosimilitud del derecho invocado y el peligro irreparable en la demora, recaudos que aparecen exigidos por el art. 15 de la Ley N.º 215, a los que se une un tercero, establecido de modo genérico para toda clase de medidas cautelares, cual es la contracautela, cabe no ser tan exigente en la apreciación del peligro del daño y viceversa ("La Ley" 1996-B-732) cuando existe el rigor de un daño extremo e irreparable, el riesgo del fumus puede atemperarse ("La Ley" 1999-A-142) las circunstancias fácticas expuestas, esta demostrada la verosimilitud del derecho invocado (conf. Fallos: 311:856, 320:521 y 2233, y sus citas, entre muchos otros como se ha establecido en distintos fallos de esta Sala).

El dictado de medidas cautelares no exige un examen de certeza sobre la existencia del derecho pretendido, sino sólo de la verosimilitud del derecho invocado. Es más, el juicio de verdad en esta materia se encuentra en oposición a la finalidad del instituto cautelar, que no es otra que atender a aquello que no excede el marco de lo hipotético, dentro del cual, asimismo, agota su virtualidad (Fallos: 315:2956; 316:2855 y 2860; 317:243 y 581; 318:30 y 532; 323:1877 y 324:2042) Asimismo, dichas medidas quedan subordinadas a la verificación de otro requisito insoslayable: el peligro irreparable en la demora y se hallan de tal modo relacionados que a mayor verosimilitud del derecho cabe no ser tan exigentes en la gravedad e inminencia del daño, y viceversa, cuando existe el riesgo de un daño de extrema gravedad e irreparable, el rigor acerca del fumus puede atenuar.

En el campo jurisdiccional, para que la viabilidad de la medida precautoria prospere los tribunales nacionales han exigido la acreditación “prima facie” de la arbitrariedad del acto cuya descalificación se persigue, o la violación de la ley, a fin de hacer caer la presunción de legalidad de que goza y, por lo tanto, suspender la ejecutoriedad del acto.

Sin perjuicio de destacar que lo expuesto hasta aquí permite considerar que en el caso existe verdadera certeza sobre la bondad del derecho alegado, no huelga recordar que la jurisprudencia de nuestro Máximo Tribunal ha sentado una importante pauta interpretativa para el análisis de este requisito al señalar que "...las medidas cautelares no exigen de los magistrados el examen de certeza sobre la existencia del derecho pretendido sino sólo su verosimilitud. Es más, el juicio de verdad en esta materia se encuentra en oposición a la finalidad de la medida cautelar, que no es otra que atender a aquello que no excede del marco de lo hipotético, dentro del cual, asimismo, agota su virtualidad" (conf. CSJN in re "Evaristo Ignacio Albornoz v. Nación Argentina Ministerio de Trabajo y Seguridad Social s/Medida de no innovar", 20/12/84, Fallos 306:2060). Por ello, estimo que V.S. debe considerar acreditada la bondad del derecho invocado.

La verosimilitud del derecho se encuentra explicitada en autos y con la documentación adjuntada, toda vez que el mismo es la supuesta colisión de normas con los principios emanados del CN, el FUMUS BONIS IURIS, surge inequívocamente de la descripción de los derechos y garantías amenazados por la ley Nº 6.339 al realizar las modificaciones mencionadas UT SUPRA.

VII.b. Peligro en la Demora.

En cuanto al peligro en la demora, como consecuencia de las situaciones perjudiciales que pueden generarse desde la sanción del acto administrativo de la Resolución N° 398/MJYSGC/19 y de seguir con las modificación realizadas por la ley Nº 6339 a la Ley Nº 5688, el derecho constitucional al debido proceso, juez natural, no discriminación, cuidado de la imagen, libertad de reunión de la sociedad en su conjunto, de periodistas y abogados, menores y adultos, sesgo discriminatorio de algoritmos que aun hoy no son evaluados ni presentados por ninguna de las partes al dejo de una ley de propiedad intelectual que impide que quienes son afectados puedan valerse de información para poder reclamar por vía ordinaria o evaluar si es o no de la forma más segura para todas las partes éste accionar intempestivo de una lesividad tan grave y manifiesta que el peligro en la demora es evidente e insoslayable. Lo mismo corre para la ley de protección

de datos personales donde los datos biométricos son considerados de los datos más sensibles que cualquier persona puede tener, uno no puede cambiar sus rasgos físicos, su caminar, su accionar normal y habitual, con los que nos lleva a tener un agente de tratamiento de datos personales sensible, sin un responsable y todas las indicaciones emitidas por la Dirección Nacional de Protección de Datos Personales como la resolución 4/2019 anexo I Criterio 4 segundo párrafo "... Los datos biométricos que identifican a una persona se considerarán datos sensibles (conforme el artículo 2°, Ley N° 25.326) únicamente cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su titular (v.g. datos que revelen origen étnico o información referente a la salud)..." Lógicamente no ha sido considerado un informe de impacto como es lo solicitado el Convenio 108 del cual Argentina es Estado parte y es una de las condiciones aceptadas para ser País Seguro ante la Unión Europea, donde cada una de las Autoridades de Control (en el caso Nacional son la Dirección Nacional de Protección de Datos Personales y la Agencia de Acceso a la Información en caso de la Ciudad Autónoma de Buenos Aires es la Defensoría del Pueblo, donde no hay informe o comunicación emitida sobre dicho informe) han seguido las más modernas legislaciones y guías en la materia, con particular atención a los Estados miembro de la Unión Europea y a los Estados parte del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personales -tratado internacional que tanto Argentina como Uruguay han suscrito y ratificado - donde estamos obligados a cumplir.

Tampoco se cumple con lo descripto en la Disposición 1/2015 de la ONTI donde se establece las buenas prácticas para el tratamiento de datos o información en cuanto a su seguridad, así mismo especifica la como mantener un nivel de seguridad en materia de "Información" y establece CÓMO se debe realizar el respectivo informe de impacto de datos personales mencionado anteriormente. Nada de esto es establecido o cumplido en cuanto se puso en práctica, ni siquiera mencionado en la ley Nº 6.339 haciendo incumplir convenios internacionales con diversos Estados y con la Unión Europea.

VII.c. No frustración del interés público.

En cuanto al requisito atinente a la no frustración del interés público, también debe dárselo por satisfecho puesto que él no puede servir de sustento para admitir la lesión cierta de derechos constitucionales ni la inobservancia del ordenamiento jurídico constitucional, en tanto el principio de legalidad obliga a la administración a actuar conforme el orden normativo vigente. Más aún, la falta de respeto del principio de legalidad atenta contra el mentado interés público, de modo tal que en la especie él debe prevalecer.

VII.d. Contracautela.

Ofrezco como contracautela la caución juratoria, en los términos y con el alcance previsto por el art 199 CPCCN.
D:

1) AFECTACIÓN CONSTITUCIONAL.
La arbitrariedad e ilegalidad del acto administrativo aquí invocado y las leyes mencionadas es de tal trascendencia que afecta la armonía y homogeneidad misma del propio texto constitucional tal como surge de lo expresado hasta el momento.

Alberdi, ya expresaba: "la ley puede ser un medio, y el más temible, de derogar las garantías que la Constitución concede. La misma Constitución pone en manos del legislador el pretexto de ejercer ese abuso por ignorancia, inconsecuencia o mal espíritu, ajeno a ella. Ni la Constitución argentina ni ninguna otra habría sido capaz de evitar este escollo, concediendo la libertad sin sujeción ni referencia a la ley. Las leyes reglamentarias de las declaraciones, derechos y garantías de los mismos son un mal necesario".

Como es sabido, es el legislador, por una parte, y el juez, por la otra, los causantes y guardianes, respectivamente, de reglamentar dichas garantías. La CN establece principios generales, reconoce derechos individuales y regla el mecanismo de los poderes de gobierno, sin que exista la posibilidad de agotar su repertorio ni poder prever todas las contingencias del futuro. Pero es la justicia la encargada de declarar cuando una ley y cualquier otro acto de autoridad es contrario a la CN, y a tal fin se deben atener no sólo a la letra de la cláusula constitucional sino que se debe analizar su espíritu.

“..los órganos del Poder Judicial deben ejercer no sólo un control de constitucionalidad, sino también 'de convencionalidad'67 ex officio entre las normas locales y la Convención Americana, evidentemente en el marco de sus respectivas competencias y de las regulaciones procesales correspondientes.68 Esta función no debe quedar limitada exclusivamente por las manifestaciones o actos de los accionantes en cada caso concreto, aunque tampoco implica que esa revisión deba ejercerse siempre, sin considerar otros presupuestos formales y materiales de admisibilidad y procedencia de ese tipo de acciones".Corte IDH, Caso Trabajadores Cesados del Congreso (Aguado Alfaro y otros) Vs. Perú, Sentencia de 24 de noviembre de 2006, párr. 128.

“..El ejercicio del control de constitucionalidad de oficio, en el marco de las competencias y regulaciones procesales correspondientes, presupone que el contralor normativo a cargo del juez se realiza en un proceso judicial ajustado a las reglas adjetivas y la descalificación constitucional se encuentra supeditada a que en el pleito quede palmariamente demostrado que irroga a alguno de los contendientes un perjuicio concreto que entraña un desconocimiento o una restricción manifiestos de alguna garantía, derecho, título o prerrogativa fundados en la Constitución, siendo la actividad probatoria de las partes así como sus planteos argumentales los que deben poner de manifiesto tal situación...Fallos: 335:2333

“...Si bien los tribunales judiciales no pueden efectuar declaraciones de inconstitucionalidad de las leyes en abstracto, es decir, fuera de una causa concreta en la cual deba o pueda efectuarse la aplicación de las normas supuestamente en pugna con la Constitución, no se sigue de ello la necesidad de petición expresa de la parte interesada, pues como el control de constitucionalidad versa sobre una cuestión de derecho y no de hecho, la potestad de los jueces de suplir el derecho que las partes no invocan o invocan erradamente -iura novit curia- incluye el deber de mantener la supremacía de la Constitución (art. 31 de la Constitución Nacional) aplicando, en caso de colisión de normas, la de mayor rango, la constitucional, desechando la de rango inferior ...(Voto del juez Carlos S. Fayt). -(Criterio sostenido en su disidencia en "Peyrú" -Fallos: 310:1401-; delineado en "Mill de Pereyra"- Fallos: 324:3219- y finalmente adoptado por la mayoría del Tribunal en "Banco Comercial de Finanzas S.A"-Fallos:327:3117-)-.

En esta senda, y ya analizando el acto impugnado corresponde mencionar que el objeto del acto administrativo consiste en lo que el acto decide, valora, certifica, registra u opina a través de la declaración pertinente. Mientras que la finalidad resulta ser el bien jurídico perseguido con el dictado del acto. Así la causa refiere a la serie de antecedentes o razones de hecho y de derecho que justifican la emisión del acto administrativo. Por su parte, el acto requiere antes de su emisión de ciertos procedimientos que lo anteceden (Hutchinson, Tomás; Régimen de Procedimientos Administrativos. Ley 19.549, 8° edición actualizada y ampliada, pág. 87/91, Ed. Astrea, Buenos Aires, 2006).-Es sabido que la actividad administrativa debe procurar la satisfacción concreta del interés público, del bien común, constituyendo esto el fin del procedimiento; por ende cualquier desviación de esa finalidad lo vicia.- Concretamente el acto debe cumplir con la finalidad que inspiró la norma por la que se otorgó competencia al órgano emisor, esto es, la pesquisa integral de los hechos objeto del sumario administrativo.-Además “La finalidad también se encuentra violentada cuando existe falta de adecuación entre los móviles que inspiraron la actuación administrativa con los queridos por la ley. Ello obliga a fiscalizar los móviles que

presidieron la actuación de los funcionarios a fin de comprobar si actuaron con una finalidad distinta de la querida por la ley" (CSJN, 23/11/95, "Laboratorios Ricar" Ed, 168-675).- Hutchinson cita entre los casos en que se viola el elemento finalidad: la irrazonabilidad, la inequidad, la violación de los principios generales del derecho y aquellos en que se persigue: 1) un beneficio personal del funcionario 2) de la administración y 3) de un tercero (CNFed Córdoba, Sala B, 30/11/89, "Menvielle Sanchez", LL, Córdoba, 1991-48).-En este sentido se reitera aquí lo expresado por Agustín Gordillo, si la decisión administrativa no se ajusta a los hechos materialmente verdaderos su acto estará viciado por esa sola circunstancia ("El acto Administrativo", Buenos Aires, 1963, pág. 136-138).-Por su parte, se pondera que la Ley de Procedimientos Administrativos exige que antes de la emisión del acto se dé cumplimiento a los procedimientos esenciales y sustanciales previstos y a los que surjan implícitos del ordenamiento jurídico (art. 7 inc. d), cuando pudiese afectar derechos subjetivos o derechos legítimos. Como sucede en el presente caso.

En los fundamentos del acto administrativo de la Resolución 398/MJYSGC/19 indican "...Que la utilización del sistema integral de video vigilancia está regida por el principio de proporcionalidad y razonabilidad, en su doble versión de procedencia y de intervención mínima. La procedencia determina que sólo podrá emplearse cuando resulte adecuado, en una situación concreta, para asegurar la convivencia ciudadana, la utilización pacífica de las vías y espacios públicos, la elaboración de políticas públicas de planificación urbana, así como para la prevención de faltas, contravenciones y delitos y otras infracciones relacionadas con la seguridad pública;Que la intervención mínima exige la ponderación en cada caso de la finalidad pretendida y la posible afectación al derecho a la propia imagen, a la intimidad y a la privacidad de las personas, de conformidad con los principios consagrados en la Constitución Nacional y la Constitución de la Ciudad Autónoma de Buenos Aires;Que la Ley Nacional Nº 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…" Los principios de proporcionalidad y razonabilidad vemos que no son cumplidos pero sí reconocidos por el Acto administrativo dado que no toma en cuenta lo vertido por las normas Nacionales y los Tratados Internacionales, cabe destacar que el artículo 5 de la Ley Nº 25.326 sobre Consentimiento, el legislador la tomó desde la Ley Española que dicho artículo ha sido declarado Inconstitucional fallo STC 2992/2000 donde el Tribunal Constitucional español detalla:

“ Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros (...) Dicha peculiaridad radica en su contenido, ya que (...), el derecho a la protección de datos atribuye a su titular un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos (..), y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales”(F.J. 6, cuarto párrafo). El fundamento jurídico 7 de la referida sentencia viene a remarcar el contenido del derecho fundamental a la protección de datos y las facultades que proporciona al individuo tanto frente al Estado como ante el particular. Dice el citado fundamento jurídico: “ De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede éste tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida , la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no , de los datos personales requiere como complementos indispensables , por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y , por otro lado, el poder oponerse a esa posesión y usos…” como bien cita el trabajo doctrinario del Magistrado Juan Manuel Fernández López (ex director de la Agencia de Protección de datos de España) en su obra titulada “El Derecho Fundamental a la Protección de Datos Personales. Obligaciones que Derivan para el Personal Sanitario”, cuyo enlace se agrega en la Prueba Documental. Como observamos la Interpretación que realiza el Gobierno de la Ciudad de Buenos Aires sobre el Artículo 5 de la Ley Nº 25.326 es erróneo y no cumple con ningún estándar de razonabilidad o proporcionalidad.

2) PRINCIPIO DE SUPREMACÍA IRRESTRICTA DE LA CONSTITUCIÓN NACIONAL ART. 31 C.N.

El artículo 31 CN establece el principio de supremacía constitucional, que determina la necesidad de subordinación de todas las normas y actos, tanto públicos como privados, a las prescripciones explícitas e implícitas contenidas en la Carta Magna.

En virtud de lo expuesto, las distintas normas y actos que se dicten o ejecuten en nuestra vida institucional deben adecuarse a las disposiciones constitucionales.

Es decir que, gobernantes y funcionarios de los tres poderes de gobierno, deben ajustar sus decisiones en las competencias que les sean pertinentes, a la letra y espíritu de la CN.

La supremacía constitucional supone una gradación jerárquica del orden jurídico derivado, que se escalona en planos distintos. Los más altos subordinan a los inferiores y todo el conjunto se debe subordinar a la Constitución. Cuando esta relación de coherencia se rompe, hay un vicio o defecto que altera la constitucionalidad del acto.

VIII. PRUEBA.

VIII.1 DOCUMENTAL.

https://www.clarin.com/tecnologia/vencio-plazo-ciberdelincuentes-publicaron-informacion-privada-robada-migraciones_0_izMLPV-xm.html

https://www.clarin.com/tecnologia/ciberdelincuentes-hackearon-argentina-gob-ar-secuestraron-50-gb-informacion-publicaran-semana_0_LU8tWEd2w.html

https://www.infobae.com/sociedad/policiales/2019/10/31/la-gorra-leaks-como-es-el-insolito-y-sencillo-truco-que-uso-un-hacker-para-robar-los-datos-privados-de-la-policia-federal/

http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

NO-2019-23068285-GCABA-DGEYTI

NO-2019-33745359-GCABA-DGEYTI

https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019

https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban

https://malegislature.gov/Bills/191/S1385

https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjSrpPI5eHtAhU0K7kGHSe-C0EQFjAFegQICBAC&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F500300.pdf&usg=AOvVaw2a9R9TIBKO2SoYkv7vnPhq

VIII.4 INFORMÁTICA.

Solicita se designe Consultor Técnico en Informática de parte al Ing Fernando Villares quien se encuentra suscripto en COPITEC al I6670, se designe Perito Informático de oficio a los fines de realizar pericial informatica en forma conjunta, según lo establecido por las Reglas del Arte.

Puntos de Pericia:

1) ¿Es posible saber cómo funciona el Sistema de Reconocimiento Facial de Prófugos?.
2) ¿Utiliza algún sistema de Inteligencia Artificial?.
3) ¿Cómo “Aprenden” los sistemas de Inteligencia Artificial?.
4) ¿Los Sistemas de Inteligencia Artificial tienen Sesgos?.
5) ¿Que mecanismos de seguridad informática deben tener los Sistemas de Reconocimiento Facial?
6) ¿El Sistema de Reconocimiento Facial de Prófugos tiene dichos sistemas de seguridad?.
7) Es obligatorio o prudente que una Empresa Privada desarrolle y controle un sistema de Identificación Biométrica de Personas?.
8) ¿Es factible saber si los datos manejados por la Empresa Privada permanecen dentro o fuera del País?.
9) ¿Existe un Sistema Informático completamente seguro para el manejo de datos tan sensibles como los Biométricos?.

10) ¿ Existe alguna herramienta de cifrado en la base de datos utilizada por la Empresa?.

11) ¿El Sistema de Reconocimiento Facial de Prófugos identifica a la totalidad de personas que son tomadas por las Cámaras para de forma posterior comparar con la Base de CONARC?.

12) ¿El Sistema de Reconocimiento Facial de Prófugos identifica a menores de edad?

13) ¿Cómo funciona el Sistema de Prevención del artículo 2 de la Ley Nº 6.339.

14) ¿El procedimiento forense descrito en el artículo 2 de la Ley Nº 6.339 cumple con las Reglas del Arte y las normativas ISO que versan sobre la Prueba Informática?.

15) ¿Es conveniente utilizar un Sistema Informático de Código Fuente Privativo o de Código Fuente Abierto?.

16) Para efectuar la carga de información de la Inteligencia Artificial se pueden utilizar imágenes de otras fuentes (RRSS) o no?.

17) Saber con qué sistema de Cifrado se encuentran trabajando, afecta a la seguridad informática del Sistema?.

Nos reservamos de ampliar puntos de pericia para el momento procesal oportuno.

IX. COMPETENCIA.

V.S. resulta competente en virtud de que el contenido normativo de art. 7° de la ley 2145, prescribe que “cuando la acción de amparo sea dirigida contra autoridades de la Ciudad, será competente para conocer el fuero Contencioso Administrativo y Tributario de la Ciudad. Como así en los términos del art 15 de la ley 2145.

X. DERECHO .

Se funda la presente demanda se funda en Derecho Constitucionales enumerados en los artículos 14, 14 bis 18, 19, 33, 43, 75 inc 22; artículos 14, 16, 18, 34, 36, 38, 39, 61 de la Constitución de la Ciudad Autónoma de Buenos Aires, en la OC 5/85 de la CIDH (Derecho a Reunión de Terceros), Pacto de San José de Costa Rica artículo 7, Pacto de Derechos Civiles y políticos en sus artículos 4, 5, 7, 9, 14, 17, 20, 21, 24, ley Nº 2.145 de la Ciudad Autónoma de Buenos Aires, Ley 1845 de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires, Ley Nº 25.326 de protección de datos personales, Convenio 108 del Consejo de Europa y jurisprudencia y derecho comparado aplicable al caso.

XI. FORMULA RESERVAS DE INCONSTITUCIONALIDAD ANTE EL TSJ Y DE REMEDIO FEDERAL ANTE LA CSJN.

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.

XII. AUTORIZA

Autorizo a compulsar el presente expediente a la Dra Maria Soledad Marinaro T°119 F° 726 del C.P.A.C.F, también se lo autoriza a la presentación y desglose de escritos y comprobantes, en especial contestaciones de demanda y peritajes, como asimismo, al diligenciamiento de cédulas, oficios, testimonios, mandamientos, retirar clave de Internet y demás diligencias de estilo que fuere menester, a sacar fotocopias del expediente y en general a realizar cualquier otra gestión que importe el impulsa de las presentes actuaciones, respecto de la cual fuere suficiente esta autorización con los límites del art.120 del C.P.C.C. y de conformidad con lo dispuesto por la acc.4/91 C.S.J.N.

XIII. PETITORIO.

Por todo lo anteriormente Expuesto Solicito:

1- Se me tenga por presentado en el carácter invocado, por parte y por constituido el domicilio procesal y electrónico

2- Se tenga por interpuesta la presente Acción de Amparo.

3- Se tenga presente el planteo del caso federal.

4- Se tengan presenten las autorizaciones conferidas.

5.- Se tenga por cumplido con el bono de derecho fijo, artículo 51, inc. d, Ley 23.187.

6.- Se haga lugar a la medida cautelar, ordenando la suspensión en la aplicación de los artículos de la Ley N.º 5.688 que reforman los artículos 478, 480, 484, 490 y las incorporaciones de los artículos 480 bis, 490 bis y de la Resolución N° 398/MJYSGC/19.

7- Oportunamente, se dicte sentencia haciendo lugar a la presente acción, con expresa imposición de costas.

PROVEER DE CONFORMIDAD

SERÁ JUSTICIA