JUZGADO DE 1RA INSTANCIA EN LO CONTENCIOSO ADMINISTRATIVO Y TRIBUTARIO Nº 23 SECRETARÍA N°45

OBSERVATORIO DE DERECHO INFORMATICO ARGENTINO O.D.I.A. CONTRA GCBA SOBRE ACCESO A LA INFORMACION (INCLUYE LEY 104 Y AMBIENTAL)

Número: EXP 9480/2019-0

CUIJ: EXP J-01-00050809-4/2019-0

Actuación Nro: 14667141/2020

Ciudad Autónoma de Buenos Aires, 20 de mayo de 2020.

VISTOS:

Los autos citados en el epígrafe en condiciones de dictar sentencia,

RESULTA:

I. A fs. 1/9 vta., se presentó el Dr. Víctor Atila CASTILLEJO ARIAS, en su carácter de apoderado del OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO y -en su representación- promovió acción de amparo contra el GOBIERNO DE LA CIUDAD DE BUENOS AIRES (en adelante, GCBA) en los términos del art. 14 de la Constitución de la Ciudad de Buenos Aires, la ley 2145 y la ley 104, a fin de que se intime al MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA a que brinde la información solicitada en su pedido de acceso a la información relacionado con la resolución 398/MJYSGC/2019, mediante la cual se aprobó la implementación en el ámbito de la Ciudad, el SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS, lo que tramitó por el expediente EX2019-21385378-GCABA-DGSOCAI.

Fundó su legitimación para realizar el pedido de información en lo establecido por el artículo 1º de la ley 104 y en tratados internacionales, así como en la jurisprudencia de la Corte Suprema de Justicia de la Nación, la Corte Interamericana de Derechos Humanos y la del fuero CAyT (fs. 1 vta./2).

Seguidamente, se refirió a la admisibilidad de la acción, afirmando que en el caso se encontraban cumplidos los cuatro requisitos establecidos por la ley 2145. En cuanto al primero, aseveró que la ley de acceso a la información pública prevé expresamente que el amparo es el medio judicial más idóneo cuando, solicitada la información a la autoridad pública, ésta omitiera entregarla sin invocar fundamento, que es lo que a su entender ocurrió en el caso. En cuanto al segundo requisito, esto es que se interponga contra un acto u omisión de alguna autoridad pública, manifestó que la nota NO-2019-25581723-GCBA-DGEYTI, de fecha 15/VIII/2019, que

le fuera notificada en fecha 27/VIII/2019 "*omitió dar respuesta a las preguntas presentadas y, consecuentemente incumplió en dar la información requerida mediante la solicitud de información pública presentada vía web*". Respecto del tercer requisito, es decir, que exista una lesión, restricción, alteración o amenaza, con arbitrariedad e ilegalidad manifiesta, de derechos y garantías, aseguró que los arts. 4º, 5º y 7º de la ley 104 imponen la obligación al GCBA de proveer la información requerida y, en caso de denegarla por alguno de los supuestos previstos en el art. 6º, la denegatoria debe estar fundada por imperativo de lo dispuesto en el art. 13 de la misma. Sin embargo, refirió que el GCBA no solo omitió proveer parte de la información requerida, sino que tampoco fundó su denegatoria para cada una de las preguntas que quedaron sin responder, incumpliendo de manera palmaria normativa aplicable y lesionando en forma arbitraria el derecho de acceso a la información. Por último, en lo que refiere al último de los requisitos -plazo de interposición de la demanda-, refirió que la Ciudad brindó su respuesta –de manera incompleta y obscura- en fecha 27/VIII/2019, por lo que el plazo de 45 días hábiles para la interposición del amparo no había transcurrido al momento de interponer la demanda. Sin perjuicio de ello, recordó la jurisprudencia del fuero ("*Gil Domínguez, Andrés c/GCBA s/acción declarativa de inconstitucionalidad*", EXP. 5296) por la cual el Tribunal Superior de Justicia declaró la inconstitucionalidad de la cláusula legal que fija dicho plazo (fs. 2 /3 vta.).

Posteriormente, manifestó que el OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO es una asociación civil sin fines de lucro que nació con el propósito de llevar adelante acciones tendientes a motivar el adecuado ejercicio y promover la defensa de los derechos constitucionales de la ciudadanía que se deriven del uso de las nuevas tecnologías. En tal sentido, alegó que persigue que el uso de estas nuevas tecnologías y los derechos derivados de ese uso sean utilizados en un marco de respeto a la democracia, los derechos humanos y los diversos grupos sociales, culturales, religiosos y étnicos (v. fs. 3 vta.).

Refirió que en fecha 25/IV/2019, con la publicación de la resolución 398/MJYSGC/2019, tomó conocimiento del sistema de reconocimiento facial implementado.

Manifestó que la aplicación de este tipo de sistemas en otras capitales del mundo fue precedida de "*un amplio y fuerte debate por parte de la ciudadanía y*

las autoridades gubernamentales", mientras que aquí el GCBA omitió llevar adelante una Evaluación de Impacto en la Privacidad (EIP), sin que sea posible determinar el impacto y la posible afectación a los datos personales y otros derechos humanos básicos de los ciudadanos de la CABA por la implementación del sistema implementado (fs. 4/4 vta.).

Asimismo, señaló que todas las preguntas efectuadas en el pedido de acceso a la información pública "*están absolutamente autorizadas por la normativa y no entran dentro de las excepciones previstas en el art. 6 de la Ley 104*" (fs. 5).

Explicó que una vez efectuada la presentación a través del portal del GCBA, recibieron dos correos electrónicos: el primero por el cual se les hizo saber que se iba verificar que su solicitud correspondiera efectivamente a un pedido de acceso a la información pública, y el segundo, a fin de informar que el pedido había sido analizado y que, efectivamente, correspondía a una solicitud de acceso a la información en los términos de la ley 104 y que sería respondido en un plazo de 15 días, pudiendo ser prorrogado por 10 días más.

Agregó que en fecha 27/VIII/ 2019, es decir 15 días después de la fecha en que debía ser evacuado el pedido, el MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA respondió en forma incompleta, parcial y deficiente a sus preguntas (fs. 5 vta.).

Junto con la demanda, acompañó en el anexo V la solicitud de acceso a la información pública presentada ante el GCBA, donde lucen las 77 preguntas efectuadas, a saber:

"1) ¿Cuántas cámaras de monitoreo posee la CABA?

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

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

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

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

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

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

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

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

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?

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

12) ¿Durante cuánto tiempo son almacenadas las imágenes capturadas por las cámaras y que procesadas a través del `Sistema de Reconocimiento Facial de Prófugos´? ¿Quién, cómo y cuándo se determina qué hacer con aquellas imágenes procesadas? ¿Dónde se las almacena? ¿Quién es propietario de aquellos servidores donde se almacenan las imágenes? ¿Cuándo, cómo y de qué manera se las abona?

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

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

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 cifrado, ¿Qué medidas de seguridad, privacidad y confidencialidad son utilizadas para asegurar su control e integridad?

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?

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?

21) Informe si el software reconoce a menores de edad

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

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

Asimismo, se ha establecido en el Art. 3 del Anexo que `[...] El Sistema de Reconocimiento Facial de Prófugos se integra con la totalidad de los registros incorporados en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC) y con los datos biométricos consultados del Registro Nacional de las Personas (RENAPER), debiendo corresponder estos últimos única y exclusivamente apersonas que registren orden judicial de restricción de la libertad registradas en la base del CONARC. Este requerimiento deberá ser dirigido a la Secretaría de Justicia y Seguridad´. Por lo que también solicitamos se nos conteste:

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

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

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 señalado en el encabezado) del convenio de confidencialidad que sería filmado 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?

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 realizan 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?

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

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 protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos? y ¿Cómo se audita su correcta destrucción?

45) ¿A través de qué sistema les llegan las alertas generada a los

Policías? ¿Qué información les son remitidas?

46) ¿Qué policías reciben esta información?

47) ¿cuántos agentes reciben esta información?

48) ¿En qué consisten estas alertas?

El Art 9 inc. 9 del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires establece que uno de los principios rectores para la implementación de las Políticas de Seguridad es la de obtener: `Información estadística confiable´: mediante la recopilación de datos relevantes en materia de seguridad sobre la base de indicadores estandarizados por el Ministerio de Justicia y Seguridad, a efectos de desarrollar informes confiables y oportunos que permitan adoptar políticas públicas eficaces en la materia. En virtud de este principio y en atención a que este Sistema de Reconocimiento Facial ha sido puesto en funcionamiento a partir del jueves 25 de abril de 2019, solicitamos se informe:

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

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?

52) ¿Cuántas de las personas detenida o demoradas con causa en el levantamiento de una alerta por el Sistema de Reconocimiento Facial, no estaban siendo buscadas por un `delito grave´? Se remite a la definición de `delito grave´ utilizada en el anexo de la resolución 1068 – E/2016.

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´?

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?

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

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

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 dc 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?

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?

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

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?

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?

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

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

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

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

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.

A efectos de mayor abundamiento solicitamos copia digital, que deberá ser remitida al correo electrónico señalado en el encabezado, la siguiente documentación:

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

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

71) Copia de la Nota NO NO-2019-09163643-DGEYFI de la Dirección General Estudios y Tecnologías de la Información determinó como Oportuna la contratación directa en virtud de 10 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 dc 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.

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 […]´...

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. ¿Cómo y qué procedimiento se para la confección de la llamada "lista negra"?

l. ¿Cuántas personas hay en esta lista?

m. ¿Cuáles el criterio que se sigue para ingresar y/ 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?

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

77) `[…] Ante eventos repetitivos, el sistema deberá enmascarar automáticamente dichos eventos a modo de optimizar la visualización de 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 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 dalos de video, registrando la información de todas las personas que aparecen, permitiendo una búsqueda dinámica y veloz de las personas de interés. […]´.

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 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´´?"

Manifestó que, en base a las respuestas brindadas por el GCBA, consideraba que habían sido respondidas únicamente las preguntas número 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 14, 43, 49, 55, 56 y 66 (fs. 6).

En relación a las restantes preguntas, las subdividió en dos grupos. En el primero, agrupó las preguntas que fueron respondidas parcialmente, ya 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". En el segundo, incluyó aquellas preguntas que directamente no fueron contestadas, sin justificación fundada (fs. 6/6 vta.).

Específicamente, respecto de las preguntas incluidas en el primer grupo, entendió lo siguiente:

*"**Pregunta N° 15:** 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:** 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 y 23:** 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:** No indicó si efectivamente existía algún convenio.*

***Pregunta 44:** El GCBA no explica qué 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:** 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 qué se refiere con `APK´.*

***Pregunta 59:** El GCBA omite totalmente responder la pregunta.*

***Pregunta 60:** 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:** 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 otro lado, cuando nos referimos al 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, VS podrá determinarlo por su propia cuenta.*

***Pregunta 63:** La pregunta estaba dirigida a averiguar a qué porcentaje de confiabilidad en una coincidencia se había comprometido la empresa y además a que indicara que porcentaje de efectividad se ha comprometido.*

***Pregunta 65:** Se utilizan términos como SLA que mi parte desconoce. Además insinúa que hay otros procesos de control que no nos ha mencionado.*

***Pregunta 67:** La pregunta estaba dirigida a 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 N° 76** y **77:** 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*" (v. fs. 6 vta./7).

En cuanto a las del segundo grupo, enumeró las preguntas que no fueron contestadas y explicó la importancia de contar con la información requerida, así refirió que:

*"**Pregunta N° 10:** 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 N° 13: *No se respondió acerca de qué manera es realizada la auditoria del borrado de las imágenes, ni tampoco cuál es la técnica de borrado utilizada.*

Preguntas N° 16 y 17: *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 N° 18, 19 y 20: *La información requerida resulta necesaria para evaluar la seguridad del sistema.*

Preguntas N° 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, y 36: *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 N° 37, 38, 39, 40, 41, 42, 46, 47 y 48: *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 N° 50 y 51: *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 N° 52 y 53: *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 N° 54, 57 y 58: *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 le Ley de Compras y Contrataciones de la Ciudad.*

Pregunta N° 64: *Es necesario conocer si existe un control por parte de la Ciudad, acerca de los compromisos asumido por la empresa.*

Requisitorias N° 25, 69, 70, 71, 72, 73, 74 y 75: *no fueron contestadas ni enviados los documentos solicitados, ni justificada dicha omisión*" (fs. 7 vta./8).

Subsidiariamente, requirió que para el caso de que este Tribunal considere que los argumentos vertidos no resultan suficientes, se solicite el acceso a la documentación requerida "*para verificar que la clasificación de la misma realizada por el GCABA haya sido realizada de acuerdo a parámetros legítimos fijados por la ley, es decir, si fue legítimamente clasificada*" dado que "*la divulgación pudiera ocasionar de manera verosímil un riesgo de seguridad pública*", conforme estipula el art. 6º, inc. e) de la ley 5784 (fs. 8 vta.).

Finalmente, ofreció prueba e hizo reserva del caso federal.

A fs. 13/80, acompañó prueba documental.

II. A fs. 83, se ordenó correr traslado de la demanda al GCBA.

A fs. 89/92, se presentó el GCBA, representado por el Dr. Diego Sebastián FARJAT, contestó demanda y solicitó el rechazo de la acción instaurada, con costas.

Preliminarmente, manifestó que a fin de cumplir con la requisitoria, previamente dio intervención a las respectivas áreas del MINISTERIO DE JUSTICIA Y SEGURIDAD para la emisión de la respuesta de su competencia, las que acompañó en soporte digital (NO-2019-33424270-GCABA-SCJS e IF-2019-33420076-GCABA-SECJS emitida por la SECRETARÍA DE JUSTICIA Y SEGURIDAD; NO-2019-33688657-DGAYCSE emitida por la DIRECCIÓN GENERAL DE ADQUISICIONES Y CONTRATACIONES DE SEGURIDAD Y EMERGENCIAS; y NO-2019-33745359-GCABA-DGEYTI emitida por la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE INFORMACIÓN).

En particular, respecto de las preguntas 24 y 25, informó que resultaba ajena a la actividad ejercida por CONARC y RENAPER, motivo por el cual no tenía el deber de contar con la información requerida, desconociendo si han suscripto convenio alguno relacionado con la transmisión de datos biométricos, asegurando que tal solicitud debería ser canalizada a través de los organismos referidos que, se encuentran en órbita

del Estado Nacional (fs. 89 vta./90).

Respecto de los puntos 28, 69, 70, 71, 73, y 75, acompañó en soporte digital:

- Copia del convenio de confidencialidad (Consulta N° 28)

- Expediente 2019-12872444-SECJS (Consulta N° 69)

- Nota NO-2019-08826279-SECJS (Consulta N° 70)

- Nota NO-2019-09163643-DGEYTI (Consulta N° 71)

- Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, los Actos administrativos de llamado y adjudicación y la respectiva Orden de Compra (Consulta N° 73)

- Copia del Convenio suscripto con la Dirección Nacional del Registro Nacional de las Personas (Consulta N° 75)

- Acto seguido, con respecto al punto 72, dijo que acompañó los pedidos de información relacionado con el sistema de reconocimiento facial de los que se tiene conocimiento, junto con sus respuestas:

- EX-2019-10600897-GCABA-DGSOCAI

- EX-2019-12276184-GCABA-DGSOCAI

- EX-2019-20597841-GCABA-DGSOCAI

- EX-2019-24827571-GCABA-DGSOCAI

- EX-2019-10513061-GCABA-MGEYA

- EX-2019- -GCABA-MGEYA

- EX-2019-33504515-GCABA-DGSOCAI (en trámite con vencimiento 4/XII/2019).

- EX-2019-33506837-GCABA-DGSOCAI (en trámite con vencimiento 4/XII/2019).

- EX-2019-31085437-GCABA-DGSOCAI (en trámite con vencimiento 11/XI/2019).

- EX-2019-32511159-GCABA-DGTALMJYS (en trámite con vencimiento 25/XI/2019).

Por último, en relación al punto 74, informó que existe convenio entre el GCBA y el CONARC, que se puede consultar en la base pública del CONARC: https://servicios.dnrec.jus.gov.ar/CONARCPublico (fs. 90 vta.).

Así, concluyó que no existía omisión por parte del GCBA y que, por el contrario, ha dado íntegra satisfacción al requerimiento efectuado por la parte actora en la primera oportunidad procesal.

III. A fs. 93, se tuvo por contestada la demanda, se ordenó el traslado a la actora de lo manifestado, reservándose por Secretaría la documental acompañada en soporte digital.

A fs. 94/99, la actora contestó el traslado conferido y manifestó que de ninguna manera consentía que, con la nueva información brindada por la demandada, pudiera tenerse por contestado el pedido de información realizado, puesto que su contraparte no sólo no contestó preguntas esenciales de su pedido, sino que obvió hacer referencia a algunos puntos claves.

Sin perjuicio de ello, manifestó que con la nueva información aportada, a las preguntas contestadas, se le deberían sumar las 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 40, 41, 42, 46, 48, 50, 51, 54, 57, 59, 60, 63, 64, 65, 68, 69, 70, 71, 72, 73, 75, con lo cual, consideró que restaría contestar las preguntas 10, 13, 20, 26, 39, 44, 45, 47, 52, 53, 58, 61, 62, 67, 74, 76 y 77.

En dicha inteligencia, expuso sus observaciones de cada una de las preguntas que consideró pendientes de respuesta. Así, dijo que:

"*Pregunta. N° 10*

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

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

Asimismo cuenta con un Convenio de Confidencialidad utilizado para la totalidad del personal del Centro de Monitoreo Urbano de acuerdo a lo normado en el artículo 483 de la Ley No 5.688/16.

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

Si bien la Administración manifiesta tener un Protocolo de Actuación sobre el Procedimiento en caso de Alerta Arrojada por el SRFP, lo cierto es que la

pregunta estaba destinada a comprender de qué manera la administración mantiene segura la información capturada hasta su destino final en el CMU.

Asimismo, si bien la Administración señala que este Protocolo de Actuación existiría, la misma no lo ha acompañado.

<u>Pregunta N° 13</u>

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

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

Como notará V.S. la administración ha obviado totalmente contestar la pregunta acerca de la técnica de borrado que debería ser utilizada al eliminar la información recopilada por las cámaras.

Tampoco ha determinado de qué manera se debería llevar a cabo la auditoría del sistema. La administración se limitó a repetir información que ya ha provisto anteriormente. Mi parte entiende que la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires es el ente que deberá auditar el sistema pero la pregunta iba dirigida a otra cuestión.

<u>Pregunta N° 20</u>

`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?´

Esta pregunta ha sido directamente obviada por el GCBA. Por lo que la administración la deberá responder.

<u>Pregunta N° 26</u>

`26) ¿A qué requerimiento se refiere la última parte del art. 3? ¿Por qué este requerimiento tiene que estar dirigido a la Secretaria de Justicia y Seguridad?´

Se ha establecido en el Art. 3 del Anexo de la Resolución 398, sobre la cual se realiza esta pregunta, que `[..] El Sistema de Reconocimiento Facial de

Prófugos se integra con la totalidad de los registros incorporados en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC) y con los datos biométricos consultados del Registro Nacional de las Personas (RENAPER), debiendo corresponder estos últimos única y exclusivamente a personas que registren orden judicial de restricción de la libertad registradas en la base del CONARC. Este requerimiento deberá ser dirigido a la Secretaría de Justicia y Seguridad.´…

Por cómo está presentado dicho articulado, no se entiende esta última expresión.

<u>Pregunta N° 39</u>

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

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

Mi parte preguntó que sucedía si la persona a la cual se detuvo no posee ninguna documentación que lo identifique. Esta pregunta está destinada a, teniendo presente que no existe norma alguna que obligue a los ciudadanos a cargar con documentación que acredite identidad, a determinar cuáles son los pasos que debe seguir el oficial cuando la persona sobre la cual se levantó una alerta no posea documentación que acredite su identidad.

El personal puede contar con cualquier sistema que se crea razonable, pero dadas las particularidades que presenta el SRFP, si no se puede determinar la identidad de la persona demorada, ¿qué sucede con el individuo?

<u>Pregunta N° 44</u>

`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 protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos y como se audita su correcta destrucción?

Teléfono institucional (POC), mediante el cual el personal policial efectúa comunicaciones respecto a necesidades operativas. Las alertas son recibidas

únicamente en los teléfonos asignados a los efectivos abocados a dicha tarea. La tecnología de estos dispositivos son Smartphone con tecnología 4G, sistema Androide, marca Samsung.

Los teléfonos institucionales no almacenan eventos.´

El GCBA no indica que tipo de aparatos se utiliza. No especifica sistema operativo, ni modelo del aparato ni a que red se conectan para el envío de la información. El hecho de que reciban eventos implica que efectivamente los reciban por lo que se deben guardar en la memoria del teléfono.

Directamente omiten establecer el protocolo de seguridad que se debiera seguir para la protección de los datos generados. Tampoco hicieron referencia alguna a si existe auditoria de esos aparatos para la eliminación de los eventos.

<u>Pregunta N° 45</u>

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

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

El hecho de que se limiten a comentar que el sistema es de desarrollo propio es nuevamente una absoluta necedad que no hace al objeto de la pregunta.

Si efectivamente es de desarrollo propio, cuál es su nombre, de qué manera se puede tener acceso a él, cuáles son las normas de seguridad y uso que le aplican. En fin, todas preguntas e inquietudes que la administración deberá contestar.

Por el otro lado, la Administración no contesta nada acerca de la información que le es remitida a los policías abocados a este SRFP.

<u>Pregunta N° 47</u>

`47) ¿Cuántos agentes reciben esta infamación?

El personal abocado por turno al servicio específico.´

Nuevamente, la pregunta hacía referencia a cuantos agentes de la policía se le envía la información de las alertas. Contestar de esta manera no hace más que hacerle perder el tiempo y esfuerzo a mi parte y a V.S.

<u>Pregunta N° 52</u>

`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 1068 - E/2016.

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

Por supuesto que el MJyS no es órgano para conceptuar o definir que es un delito grave. Precisamente por esa razón nos remitimos a la Resolución 1068 — E/2016 que conceptualiza dicha definición en el marco del Registro Nacional de Reincidencia que creara el CONARC.

Lo cierto es que el MJyS es el único que puede determinar cuántas personas han sido detenidas con causa en una alerta levantada por el SRFP y que a su vez nos pueda decir cuántas de ellas no eran buscadas por un "delito grave" en los términos de la resolución mencionada.

Dicho esto, la normativa es aplicable a todos y que la Administración manifieste desconocer una Resolución de un organismo Federal es verdaderamente asombroso.

<u>Pregunta N° 53</u>

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

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

La Administración se limita a dar información ya provista. Nos remitimos a los mismos argumentos señalados en la pregunta anterior.

<u>Pregunta N° 58</u>

`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 pregunta no ha tenido respuesta alguna. Pregunta N' 61

`61) ¿Qué método de detección de rostros se utilizó? En caso de utilizar redes neuronales, ¿qué modelo/arquitectura se utilizó y cuál lite el set de datos que se

utilizó para entrenar el modelo?

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

El objeto de esta pregunta no se encuentra destinado a saber información protegida por derechos de propiedad intelectual de la empresa adjudicataria.

En los sistemas de reconocimiento facial se suelen utilizar distintos métodos de detección de rostros los cuales tienen nombres técnicos como holísticos, locales o geométricos.

Así, otros ejemplos de métodos que son el Análisis de Componentes Principales (PCA - Principal Component Analysis), el Análisis Linear Discriminante (LDA - Linear Discriminant Analysis) o el Discriminante Linear de Fisher (FLD Fisher Linear Discriminant).

Esta información no tiene por qué estar protegida por copyright ya que es información técnica del producto que no es original del que provee el servicio si no que es meramente descriptiva del método que utilizaría el mismo.

Por el otro lado, el set de datos utilizado para entrenar el producto tampoco debería ser información protegida por copyright ya que la misma debería haber sido entrenada con imágenes de ciudadanos. A no ser que el mismo haya sido entrenado con imágenes de ciudadanos de otros países, lo cual hablaría bastante de la eficacia que un sistema entrenado con imágenes de un país de con una demografía distinta a la nuestra, pero que de igual no estaría protegida por el copyright.

<u>Pregunta N° 62</u>

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

Ver respuesta 61.´

Nos remitimos a los comentarios de la pregunta 61.

<u>Pregunta N° 67</u>

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

Conforme la Resolución 398/2019, la Defensoría del Pueblo de la

Ciudad Autónoma de Buenos Aires es el organismo auditor´.

La administración no contesta la pregunta la cual fue directamente esquivada. Lo que mi parte quiere saber es si se realizó una auditoria del sistema o no. Bastante sencillo.

<u>Pregunta N° 74</u>

`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.´

En el escrito de contestación de demanda la Administración dice: `Por último, en relación al punto 74, se informa que existe convenio entre el Gobierno de la Ciudad de Buenos Aires y el CONARC.

A todo evento se hace saber el link de la base pública del CONARC: https://servicio.dnrec.jus.gov.ar/CONARCPublico´.

Sin embargo, la administración NO acompañó la copia del convenio solicitado por lo que se insiste nuevamente en su remisión.

<u>Pregunta N° 76 y N° 77</u>

Como dicha pregunta tiene una extensión considerable nos remitimos a la misma que se podrá encontrar en el Anexo V de la demanda.

A estas preguntas el estado contestó:

`Lo enunciado en los párrafos previos, no corresponden a características técnicas del Sistema de Reconocimiento Facial de Prófugos. Estos conceptos devienen de la adquisición de otros software (predictivo y forense).´ Sin embargo, estos conceptos, como podrá ver V.S, se encuentran en el PLIEGO DE BASES Y CONDICIONES PARTICULARES. CONTRATACIÓN DIRECTA DE UN SERVICIO DE ANÁLISIS INTEGRAL DE VIDEO. Que ya ha acompañado el estado y que mi parte ha presentado como Anexo XI. Dicho pliego es que se utilizó a efectos de realizar la compra del SRFP.

Más precisamente dichas expresiones se pueden encontrar en las especificaciones técnicas del mismo que empezarían en la página 38 en adelante bajo el punto `2.2.1. Especificaciones técnicas.´

Por lo tanto, solicitamos que V.S. intime a la parte demandada a que dé respuesta a dichas preguntas de manera completa, veraz y adecuada" (fs. 94 vta./98).

IV. A fs. 100, se dispuso el traslado a la demandada de la contestación de la actora, que lo contestó a fs. 104/118 vta.

En primer término, manifestó acompañar la nota NO-2019-37210893-GCBA-DGALSE, por la cual la DIRECCIÓN GENERAL ADMINISTRATIVA DE SEGURIDAD Y EMERGENCIA del MINISTERIO DE JUSTICIA Y SEGURIDAD de la Ciudad, acompañó las notas NO-2019-3366393-GCABA-DGALSE, NO-2019-36874307-GCABA-SECJS, NO-201936876659-GCABA-SECJS, NO-2019-36772362-GCABA-SIOOU, NO-2019-37151628-DGAYCSE y NO-2019-37063734-GCABA-DGEYTI, mediante las que, según dijo, las áreas competentes del referido Ministerio, brindaron la información requerida por la actora en la presentación que motivó el traslado.

V. A fs. 119, se dispuso el traslado de la contestación del GCBA y de la documental acompañada, el que fue contestado por la actora a fs. 120/125 vta.

En primer término, manifestó que con las respuestas brindadas en esta nueva oportunidad por el GCBA, daba por contestadas las preguntas 39 y 74.

Acto seguido, expuso sus observaciones de cada una de las preguntas que consideró pendientes de respuesta. Así, dijo que:

"Pregunta N° 10

`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?

Respuesta 1er. Traslado: El Centro de Monitoreo Urbano (CMU) cuenta con un Protocolo de actuación sobre el Procedimiento en caso de alerta arrojada por el `Sistema de Reconocimiento Facial de Prófugos´.

Asimismo cuenta con un Convenio de Confidencialidad utilizado para la totalidad del personal del Centro de Monitoreo Urbano de acuerdo a lo normado en el artículo 483 de la Ley N° 5.686.

Por último, el C.A.P1 implementó la gestión de seguimiento de calidad respecto al sistema de reconocimiento facial de prófugos´.

***Mi parte manifestó en su primera contestación de traslado:** Si bien la. Administración manifiesta tener un Protocolo de Actuación sobre el Procedimiento en caso de Alerta Arrojada por el SRFP, lo cierto es que la pregunta estaba destinada a comprender de qué manera la administración mantiene segura la información*

capturada hasta su destino final en el CMU.

Asimismo, si bien la Administración señala que este Protocolo de Actuación existiría, la misma no lo ha acompañado.

<u>Respuesta 2do traslado de la Administración:</u> La información desde que es capturada hasta que llega al CMU viaja encriptada mediante aplicabilidad de protocolo 3DES.

Como podrá advertir V.S. el GCBA no compartió el Protocolo al que hizo referencia en, su primera respuesta.

De esta manera, V.S. deberá intimar al estado a. proveer el supuesto protocolo que manifiestan tener.

<u>Pregunta N° 13</u>

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

<u>Respuesta 1er Traslado de la Administración:</u> La auditoría del funcionamiento del Sistema de Reconocimiento Facial de Prófugos es llevada a cabo por la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires. El sistema de referencia no almacena imágenes a excepción de las alertas correspondiente a aquellas personas buscadas por la justicia. Conforme a lo enunciado, las imágenes que no devienen en una alerta positiva son automáticamente descartadas de/proceso de almacenamiento del sistema.´

***Mi parte manifestó en su primera contestación de traslado:** Como notará V.S. la administración ha obviado totalmente contestar la pregunta acerca de la técnica de borrado que debería ser utilizada al eliminar la información recopilada por las cámaras.*

Tampoco ha determinado de qué manera se debería llevar a cabo la auditoria del sistema. La administración se limitó a repetir información que ya ha provisto anteriormente. Mi parte entiende que la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires es el ente que deberá auditar el sistema pero la pregunta iba dirigida a otra cuestión.

<u>Respuesta 2do traslado de la Administración:</u> Como ya hemos respondido oportunamente, el SRFP no almacena imágenes de las lecturas realizadas, excepto sea una lectura positiva. Es decir, que la persona se encuentra en la base de

datos del CONARC impartida por la justicia. En estos casos, estas imágenes reciben el mismo tratamiento que el estipulados en la Ley original N. 2602/08 abrogada por la ley 5688/16.

La pregunta nuevamente no ha sido contestada. No se ha hecho referencia alguna a la técnica de borrado de las imágenes. Es evidente que si las imágenes son trasladas desde la captura de la imagen en las cámaras al CMU que aunque sea provisoriamente, dichas imágenes deben ser almacenadas en algún elemento físico. Existen distintas técnicas de borrados tales como la desmagnetización, destrucción física, sobre-escritura,, métodos de borrado provistos por el mismo sistema y que pueden ser altamente inseguros, etc.

Pregunta N° 20

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

Mi parte manifestó en su primera contestación de traslado: *Esta pregunta ha sido directamente obviada por el (CBA. Por lo que la administración la deberá responder.*

Respuesta 2do traslado de la Administración: A través de la Nota NO-2019- 36772362-GCABA-SIOOU el Estado manifestó `[...] que por medio del presente se informa que se han ingresado un total de 43 altas al Sistema de Reconocimiento Facial de Prófugos por requerimiento judicial [...]´.

Mi parte no tiene manera de determinar si dicha respuesta está orientada a esta pregunta pero en el caso que así sea debo destacar que en ningún momento se aclara si dichas altas corresponden a altas en la Base de Datos del CONARC o si directamente utilizaron datos provistos por estos "requerimientos judiciales" para hacer una especie de alta manual en el SRFP.

Pregunta N° 26

`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?´

Mi parte manifestó en su primera contestación de traslado: *Se ha establecido en el Art 3 del Anexo de la Resolución 398, sobre la cual se realiza esta pregunta, que `[...] El Sistema de Reconocimiento Facial de Prófugos se integra con la*

totalidad de los registros incorporados en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC) y con los datos biométricos consultados del Registro Nacional de las Personas' (RENAPER), debiendo corresponder estos últimos única y exclusivamente a personas que registren orden judicial de restricción de la libertad registradas en la base del CONARC. ***Este requerimiento deberá ser dirigido a la Secretaría de Justicia y Seguridad****.´ (lo destacado es nuestro).*

Por cómo está presentado dicho articulado, no se entiende esta última expresión.

Respuesta 2do traslado de la Administración: -

Dicha respuesta brilla por su ausencia. La administración nuevamente obvia totalmente a realizar expresión alguna sobre dicha pregunta.

<u>Pregunta Nº 44</u>

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

<u>Respuesta 1er Traslado de la Administración</u>: Teléfono institucional (POC), mediante el cual el personal policial efectúa comunicaciones respecto a necesidades operativas. Las alertas son recibidas únicamente en los teléfonos asignados a los efectivos abocados a dicha tarea. La tecnología de estos dispositivos son Smartphone con tecnología 4G, sistema Androide, marca Samsung.

Los teléfonos institucionales no almacenan eventos.´

Mi parte manifestó en su primera contestación de traslado: *El GCBA no indica qué tipo de aparatos se utiliza, no especifica sistema operativo, ni modelo del aparato ni a qué red se conectan para el envío de la información. El hecho de que reciban eventos implica que efectivamente los reciban por lo que se deben guardar en la memoria del teléfono.*

Directamente omiten establecer el protocolo de seguridad que se debiera seguir para la protección de los datos generados. Tampoco hizo referencia alguna a si existe auditoría de esos aparatos para la eliminación de los eventos.

<u>Respuesta 2do traslado de la Administración:</u> Como se mencionara

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

El estado sigue sin contestar si se realiza una auditoría de estos aparatos para determinar si la información es efectivamente borrada.

<u>Pregunta N° 45</u>

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

<u>Respuesta ler Traslado de la Administración</u>: Las alerta llegan a los efectivos asignados a dicha función mediante una APP (aplicación) especifica de desarrollo propio, la cual posee normas de seguridad y uso (control de logging, y marca de agua en usuarios).”

***Mi parte manifestó en su primera contestación de traslado:** El hecho de que se limiten a comentar que el sistema es de desarrollo propio es nuevamente una absoluta necedad que no hace al objeto de la pregunta.*

Si efectivamente es de desarrollo propio, cuál es su nombre, de qué manera se puede tener acceso a él, cuáles son las normas de seguridad y uso que le aplican. En fin, todas preguntas e inquietudes que la administración deberá contestar.

Por el otro lado, la Administración no contesta nada acerca de la información que le es remitida a los policías abocados a este SRFP.

<u>Respuesta 2do traslado de la Administración</u>: Como ya se mencionara, los teléfonos institucionales provistos reciben alertas a través de una ampliación donde enuncia; la foto de la persona prófuga de la justicia, número de cámara de video que la detectó y toda aquella información de la causa judicial extraída del CONARC.

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

Nuevamente el estado omite identificar efectivamente la aplicación utilizada.

Pregunta N° 47

`47) ¿Cuántos agentes reciben esta información?

Respuesta ler Traslado de la Administración: El personal abocado por turno al servicio específico´.

Mi parte manifestó en su primera contestación de traslado: *Nuevamente, la pregunta hacía referencia a cuantos agentes de la policía se le envía, la información de las alertas. Contestar de esta manera no hace más que hacerle perder el tiempo y esfuerzo a mi parte y a V.S.*

Respuesta 2do traslado de la Administración:

El estado no contesta la pregunta que se le realiza

Pregunta N ° 52

`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 1068 - E/2016,

Respuesta ler Traslado de la Administración: El MJyS no es órgano competente para conceptuar o definir los delitos graves.´

Mi parte manifestó en su primera contestación de traslado: *Por supuesto que el MJyS no es órgano para conceptuar o definir que es un delito grave. Precisamente por esa razón nos remitimos a la Resolución 1068 - E/2016 que conceptualiza dicha definición en el marco del Registro Nacional de Reincidencia que creara el CONARC.*

Lo cierto es que el MJyS es el único que puede determinar cuántas personas han sido detenidas con causa en una alerta levantada por el SRFP y que a su vez nos pueda decir cuántas de ellas no eran buscadas por un "delito grave" en los términos de la resolución mencionada.

Dicho esto, la normativa es aplicable a todos y que la Administración manifieste desconocer una Resolución de un organismo Federal es verdaderamente asombroso.

Respuesta 2do traslado de la Administración: El estado no contesta la pregunta.

Pregunta N ° 53

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´?

Respuesta ler Traslado de la Administración: A la actualidad 1648 personas han sido identificadas y puestas a disposición de la justicia.

***Mi parte manifestó en su primera contestación de traslado:** La Administración se limita a dar información ya provista. Nos remitimos a los mismos argumentos señalados en la pregunta anterior.*

Respuesta 2do traslado de la Administración: El estado no contesta la pregunta.

Pregunta N° 58

`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?´

Respuesta ler Traslado de la Administración:

***Mi parte manifestó en su primera, contestación de traslado:** La pregunta no ha tenido respuesta alguna.*

Respuesta 2do traslado de la Administración: El estado no contesta la pregunta.

Pregunta Nº 61

`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?

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

***Mi parte manifestó en su primera contestación de traslado:** El objeto de esta pregunta no se encuentra destinado a saber información*

protegida por derechos de propiedad intelectual de la empresa adjudicataria.

En los sistemas de reconocimiento facial se suelen utilizar distintos métodos de detección de rostros los cuales tienen nombres técnicos como bolis- ticos, locales o geométricos.

Así, otros ejemplos de métodos que son el Análisis de Componentes Principales (PCA - Principal Component Analysis), el Análisis Linear Discriminante (LDA - Linear Discriminant Analysis) o el Discriminante Linear de Fisher (FLD Fisher Linear Discriminant).

Esta información no tiene por qué estar protegida por copyright ya que es información técnica del, producto que no es original del que provee el servicio si no que es meramente descriptiva del método que utilizaría el mismo.

Por el otro lado, el set de datos utilizado para entrenar el producto tampoco debería ser información protegida por copyright ya que la misma debería haber sido entrenada con imágenes de ciudadanos. A no ser que el mismo haya sido entrenado con imágenes de ciudadanos de otros países, lo cual hablaría bastante de la eficacia que un sistema entrenado con imágenes de un país de con una demografía distinta a la nuestra, pero que de igual manera no estaría protegida por el copyright.

<u>Respuesta 2do traslado de la Administración</u>: Dependiendo de la calidad de las imágenes obtenidas del cruzamiento de la base de datos de CONARC con el RENAPER, se utiliza alguno de los métodos siguientes: holístico, locales o Geométricos.

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

El estado confirma que utilizaron, distintos sujetos de prueba pero no aporta a la causa aquellos datos para poder evaluar la idoneidad de esos datos para su entrenamiento.

<u>Pregunta N° 62</u>

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

Respuesta ler Traslado de la Administración: Ver respuesta 6.1.´

***Mi parte manifestó en su primera contestación de traslado**: Nos remitirnos a los comentarios de la pregunta 61.*

Respuesta 2do traslado de la Administración: Como set de datos para calibrar y verificar el funcionamiento del sistema, se realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los casos los porcentajes de error exigidos.

La administración no identifica cuál fue el dataset utilizado para el entrenamiento de este Sistema.

Pregunta Nº 67

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

Respuesta ler Traslado de la Administración: Conforme la Resolución 398/2019, la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires es el organismo auditor´.

***Mi parte manifestó en su primera contestación de traslado:** La administración no contesta la pregunta la cual fue directamente esquivada. Lo que mi parte quiere saber es si se realizó una auditoría del sistema o no. Bastante sencillo,*

Respuesta 2do traslado de la Administración: Conforme a la resolución 398/2019 en su artículo 3, se invita a la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires a auditar el funcionamiento del SRFP, a cuyo fin se concluyeron reuniones informativas y demostrativas de procedimientos reales en el Centro de Monitoreo Urbano - Centro Operativo del SRFP.

Asimismo, se remitió la información técnica requerida a la Defensoría del Pueblo [acerca del] *funcionamiento técnico y operativo del SRFP.*

Nuevamente, el Estado evita confirmar o negar si se realizó alguna auditoría del sistema.

Pregunta N° 76 y N° 77

Como dicha pregunta tiene una extensión considerable nos remitimos a la misma que se podrá encontrar en el Anexo V de la demanda.

Respuesta ler Traslado de la Administración: "Lo enunciado en los párrafos previos, no corresponden a características técnicas del Sistema de Reconocimiento Facial de Prófugos. Estos conceptos devienen de la adquisición de otros software (predictivo orense)."

Mi parte manifestó en su primera contestación de traslado: *Sin embargo, estos conceptos, como podrá ver V.S., se encuentran en el PLIEGO DE BASES Y CONDICIONES PARTICULARES, CONTRATACIÓN DIRECTA DE UN SERVICIO DE ANÁLISIS INTEGRAL DE VIDEO. Que ya ha acompañado el estado y que mi parte ha presentado como Anexo XI. Dicho pliego es que se utilizó a efectos de realizar la compra del SRFP. Más precisamente dichas expresiones se pueden encontrar en las especificaciones técnicas del, mismo que empezarían en la página 38 en adelante bajo el punto "2.2.1. Especificaciones técnicas".*

Por lo tanto, solicitamos que V.S. intime a la parte demandada a que dé respuesta a dichas preguntas de manera completa, veraz y adecuada.

Respuesta 2do traslado de la Administración: El pliego de bases y condiciones mencionado, incluía dos sistemas, es SRFP y un sistema de análisis forense de imágenes y predictivo. Todas las preguntas solicitadas en estos puntos, corresponden a los sistemas mencionados en segunda instancia, los cuales no son objeto de/presente requerimiento" (fs. 120/125 vta.).

VI. A fs. 127, la actora solicitó se resolviera, por lo que a fs. 128 quedaron las actuaciones en condiciones de resolver.

Y CONSIDERANDO:

I. En primer término, corresponde efectuar una apreciación preliminar respecto a la legitimación invocada por la asociación actora.

En tal sentido, es necesario recordar que la Constitución de la Ciudad garantiza "[e]*l acceso a la justicia de todos sus habitantes*" (conf. art. 12, inciso 6, de la CCABA) y promueve la remoción de "*los obstáculos de cualquier orden que, limitando de hecho la igualdad y la libertad, impidan la efectiva participación en la vida política, económica o social de la comunidad*" (conf. art. 11 de la CCABA). Específicamente, al regular el amparo, establece que "[t]*oda persona puede ejercer acción expedita, rápida y gratuita de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares que en forma actual o*

inminente, lesione, restrinja, altere o amenace con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por la Constitución Nacional, los tratados internacionales, las leyes de la Nación, la presente Constitución, las leyes dictadas en su consecuencia y los tratados interjurisdiccionales en los que la Ciudad sea parte" (conf. art. 14 primer párrafo de la CCABA) y agrega que "[e]*stán legitimados para interponerla cualquier habitante y las personas jurídicas defensoras de derechos o intereses colectivos, cuando la acción se ejerza contra alguna forma de discriminación, o en los casos en que se vean afectados derechos o intereses colectivos, como la protección del ambiente, del trabajo y la seguridad social, del patrimonio cultural e histórico de la Ciudad, de la competencia, del usuario o del consumidor*" (conf. art. 14 segundo párrafo de la CCABA).

Es decir que la Constitución porteña reconoce una legitimación amplia a cualquier habitante, aun cuando no ostentara un interés legítimo o un derecho subjetivo, para acceder a la justicia mediante el amparo.

Ello resulta concordante con el criterio establecido por el legislador local, en la ley 104 de acceso a la información pública, publicada en el BOCBA 600 del 29/XII/1998, que determina que "**[t]*oda persona*** *tiene derecho a solicitar y a recibir información completa, veraz, adecuada y oportuna. Para ejercer el derecho de acceso a la información pública no será necesario acreditar derecho subjetivo, interés legítimo o razones que motiven la petición*" y que "[i]*mplicará la libertad de acceder, solicitar, recibir, copiar, analizar, reprocesar y redistribuir información bajo custodia de los sujetos obligados, con las únicas limitaciones y excepciones que establece la presente ley*" (conf. art. 1º, el destacado es propio).

La locución empleada en el texto, esto es, la titularidad del derecho de "*toda persona*" a obtener la información, transmite claramente la voluntad de inclusión del legislador de cualquier habitante para promover la acción de amparo (CCAyT, Sala I, 29/11/2000, "*Defensoría del Pueblo de la Ciudad de Buenos Aires c/Secretaría de Obras y Servicios Públicos s/Amparo*", EXP 9903/0; 04/IX/2002 "*Baltroc, Beatriz Margarita c/G.C.B.A. s/Amparo*", EXP 4324/0).

A título ilustrativo, cabe recordar que dicho criterio también ha sido el seleccionado a nivel nacional, mediante la ley 27.275, publicada en el BO 33472 del 29/IX/2016, cuyo art. 4° enuncia la legitimación activa en los siguientes términos:

"**[t]*oda persona humana o jurídica, pública o privada,*** *tiene derecho a solicitar y recibir información pública, no pudiendo exigirse al solicitante que motive la solicitud, que acredite derecho subjetivo o interés legítimo o que cuente con patrocinio letrado*".

Cabe recordar que la Corte Suprema de Justicia de la Nación ha sostenido que, conforme el criterio sentado por la Corte IDH en "*Claude Reyes*", el artículo 13 de la Convención Americana sobre Derechos Humanos, "*al estipular expresamente los derechos `buscar´ `recibir´ `informaciones´, protege el derecho que tiene toda persona solicitar el acceso la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención*", por lo que dicho artículo "*ampara el derecho de las personas recibir dicha información la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso conocer esa información reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso la misma para el caso concreto*", y que dicha información "*debe ser entregada sin necesidad de acreditar un interés directo para su obtención una afectación personal, salvo en los casos en que se aplique una legitima restricción*". Ello en atención a la doble dimensión del derecho de acceso la información bajo el control del Estado, individual y social, que "*deben ser garantizadas por el Estado de forma simultánea*" (CSJN, 04/XII/2012, "*Asociación Derechos Civiles c/E.N. PAMI dto. 1172/03 s/amparo ley 16986*", 04/XII/2012, *Fallos*: 335:2393, consid. 9º).

Ahora bien, en el caso, se trata de una asociación civil que declaró estar debidamente inscripta en el REGISTRO PÚBLICO DE COMERCIO de la INSPECCIÓN GENERAL DE JUSTICIA, bajo el número 213, libro 2AC de Asociaciones Civiles, dedicada a la defensa de los derechos constitucionales que se deriven del uso de las nuevas tecnologías, y que persigue que el uso de estas nuevas tecnologías y los derechos derivados de ese uso sean utilizados en un marco de respeto a la democracia, los derechos humanos y los diversos grupos sociales, culturales, religiosos y étnicos (v. fs. 1, 3 vta./4).

En virtud de la calidad invocada por la parte actora y los derechos invocados, tengo para mí que se encuentra suficientemente satisfecho el presupuesto de la acción vinculado con la legitimación activa.

II. Reconocida la legitimación activa invocada por la parte actora,

razones de orden lógico imponen que se evalúe, en segundo término, la admisibilidad formal de la vía intentada.

La parte actora interpuso demanda de amparo por acceso a la información pública en los términos de lo dispuesto en el art. 14 de la CCABA y las leyes 104 y 2145, con el objeto de que se condene al GCBA a brindar información relativa al SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS, cuya implementación fue aprobada por la resolución 398/MJYSGC/2019.

Refirió que debió acudir a la justicia luego de efectuar una petición administrativa, que tramitó por el expediente administrativo EX2019-21385378-GCABA-DGSOCAI, que a su entender no fue satisfecha adecuada ni integralmente por el GCBA.

A efectos de evaluar la admisibilidad de la vía de amparo por acceso a la información pública intentada, corresponde detenerme en la normativa que regula el asunto.

En tal sentido, como se señaló anteriormente, el art. 14 de la Constitución de la Ciudad consagra en su que "[t]*oda persona puede ejercer acción expedita, rápida y gratuita de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares que en forma actual o inminente, lesione, restrinja, altere o amenace con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por la Constitución Nacional, los tratados internacionales, las leyes de la Nación, la presente Constitución, las leyes dictadas en su consecuencia y los tratados interjurisdiccionales en los que la Ciudad sea parte…*".

Asimismo, la ley 2145, publicada en el BOCBA 2580 del 05/XII/2006, reglamentaria de dicho art. 14 de la CCABA, prescribe que "[l]*a acción de amparo es expedita, rápida y gratuita y procede, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente, lesione, restrinja, altere o amenace con arbitrariedad e ilegalidad manifiesta, derechos y garantías reconocidos por la Constitución Nacional, los tratados internacionales, las leyes de la Nación, la Constitución de la Ciudad Autónoma de Buenos Aires, las leyes dictadas en su consecuencia y los tratados interjurisdiccionales en los que la Ciudad sea parte…*".

Por su parte, la ley 104, publicada en el BOCBA 600 del 29/XII/1998,

t.c. 2018, determina que "[t]*oda persona tiene derecho a solicitar y a recibir información completa, veraz, adecuada y oportuna. Para ejercer el derecho de acceso a la información pública no será necesario acreditar derecho subjetivo, interés legítimo o razones que motiven la petición*" y que "[i]*mplicará la libertad de acceder, solicitar, recibir, copiar, analizar, reprocesar y redistribuir información bajo custodia de los sujetos obligados, con las únicas limitaciones y excepciones que establece la presente ley*" (conf. art. 1º).

A su vez, el art. 12 prevé que "[e]*n caso que el/la peticionante considere que su solicitud de información no hubiere sido satisfecha o si la respuesta a la requisitoria hubiere sido ambigua o parcial, podrá considerarlo como negativa injustificada a brindar información, quedando habilitada la vía de reclamo prevista en la presente ley* ***o la Acción de Amparo ante el fuero Contencioso Administrativo de la Ciudad Autónoma de Buenos Aires***" (el destacado es propio).

A la luz de la normativa transcripta, emerge con claridad que la vía del amparo es la prescripta expresamente para los casos como el presente, donde a entender del o la peticionante de información pública, la respuesta brindada resulta ambigua o parcial, sin hallar justificación legítima para ello.

Vale la pena recordar que "[l]*a acción de amparo es una acción principal. Ni es subsidiaria, ni es heroica, ni es residual ni es de excepción, y sólo cede ante la existencia de un medio exclusivamente judicial, más idóneo, esto es, más expeditivo y rápido (conforme las Conclusiones de la comisión n° 3, en el XIX Congreso Nacional de Derecho Procesal en materia de amparo). Por vía del amparo se realiza tanto el fin preventivo como el inhibitorio, propios de la función jurisdiccional, la cual, como está reconocido desde hace décadas en la doctrina y en el derecho comparado, no se agota en su dimensión represiva (vg. mandato de injunção en Brasil, y, los llamados prohibitory injuction y mandatory injuction, en el modelo del common law)*" (TSJ, 26/XII/2000, "*T.S. c/GCBA s/amparo*", del voto de la Dra. RUIZ). En similar sentido, se hallan numerosos pronunciamientos, entre los cuales se destacan: CCAyT, Sala I, 11/XII/2001, "*Del Piero Fernando Gabriel c/GCBA s/ejecución de sentencias contra autoridad administrativa*"; Sala II, 13/III/2001, "*Pujato, Martín Raúl c/GCBA s/amparo*" y 23/II/2001, "*Ermini, Enrique Bernardino c/GCBA s/amparo*".

A mayor abundamiento, cabe recordar que la Corte Suprema de Justicia

de la Nación ha recordado que "*en materia de protección judicial del derecho al acceso la información en poder del Estado, la CIDH ha enfatizado... `la necesidad de que exista un* ***recurso sencillo, rápido efectivo*** *para determinar si se produjo una violación al derecho de quien solicita información y, en su caso, ordene al órgano correspondiente la entrega de la información. Para ello se debe tomar en cuenta que es práctica corriente la negativa suministrar la información que se solicita las instituciones el silencio ante un pedido que la celeridad en la entrega de la información es indispensable en esta materia"*" (CSJN, 04/XII/2012, "*Asociación Derechos Civiles c/E.N. PAMI dto. 1172/03 s/amparo ley 16986*", 04/XII/2012, *Fallos*: 335:2393, considerando 10, el destacado es propio).

En efecto, tales han sido los términos y las circunstancias en que la demanda fue impetrada, sin que -por otra parte- la demandada hubiera cuestionado la idoneidad de la vía elegida.

En virtud de tales consideraciones, estimo que la vía del amparo elegida por la actora para acceder a la información pública resulta admisible.

III. A efectos de resolver la controversia suscitada entre las partes, habrá que delimitar sus contornos.

Se trata de un amparo por acceso a la información pública impetrado por el OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO, luego de tramitar en sede administrativa una petición de información pública respecto del SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS, cuya implementación fue aprobada por la resolución 398/MJYSGC/2019, que tramitó por el expediente administrativo EX2019-21385378-GCABA-DGSOCAI, que a su entender no fue satisfecha adecuada ni integralmente por el GCBA.

Éste, por su parte, alegó haber dado suficiente respuesta a cada uno de los interrogantes planteados, por lo que solicitó el rechazo de la demanda, con costas.

Ahora bien, desde la petición administrativa de acceso a la información pública consistente en 77 preguntas, la actora fue dando por respondidas la mayoría de ellas a lo largo tiempo, sea en sede administrativa o durante la tramitación de la presente causa.

En tal sentido, cabe señalar que al momento de interponer la demanda, la propia actora manifestó que del pedido de acceso a la información pública tramitada en

sede administrativa, daba por satisfecha la respuesta brindada por la Administración a las preguntas 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 14, 43, 49, 55, 56 y 66 (fs. 6). Es decir que dichas preguntas no integran la *litis*.

Luego, en su presentación de fs. 94/99, la actora también tuvo por contestadas las preguntas 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 40, 41, 42, 46, 48, 50, 51, 54, 57, 59, 60, 63, 64, 65, 68, 69, 70, 71, 72, 73 y 75; ello con motivo de la respuesta brindada por el GCBA al contestar la demanda (v. fs. 89/92).

Del mismo modo, a fs. 120/125, la actora tuvo por contestadas las preguntas 39 y 74, en atención a la respuesta brindada por el GCBA a fs. 104/118 vta.

En atención a la reseña hasta aquí efectuada, corresponde declarar abstracta la cuestión traída a conocimiento de este Tribunal relacionada con las preguntas 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 46, 48, 50, 51, 54, 57, 59, 60, 63, 64, 65, 68, 69, 70, 71, 72, 73, 74 y 75.

En consecuencia, el marco de dilucidación que corresponde a este Tribunal se limitará a las preguntas 10, 13, 20, 26, 44, 45, 47, 52, 53, 58, 61, 62, 67, 76 y 77.

IV. Una vez delimitado el objeto de la presente controversia, corresponde reseñar el régimen normativo aplicable.

En tal sentido, cabe señalar que el derecho de acceso a la información pública encuentra su fundamento en normas del más alto rango de nuestro ordenamiento jurídico, erigiéndose como un componente sustancial de las instituciones democráticas.

IV.1. Así, la Constitución nacional garantiza el principio de publicidad de los actos de gobierno y el derecho de acceso a la información pública a través de los artículos 33, 41 y 42.

Asimismo, el derecho de buscar y recibir información encuentra recepción normativa en la Declaración Americana de Derechos Humanos (artículo 4°), la Convención Americana sobre Derechos Humanos (artículo 13.1), la Declaración Universal de Derechos Humanos (artículo 19) y el Pacto Internacional de Derechos Civiles y Políticos (artículo 19 inc. 2), entre otros tratados internacionales de derechos humanos con jerarquía constitucional (conf. artículo 75, inc. 22 CN).

En tanto dichos tratados deben ser interpretados a la luz de los estándares interpretativos elaborados por los órganos de aplicación e interpretación de los mismos a fin de cumplir con la manda constitucional y aplicarlos *en las condiciones de su vigencia* (conf. *Fallos:* 318:514; 319:1840; 327:3753; 332:709), corresponde recordar algunos importantes precedentes en la materia.

En el caso "*Claude Reyes y otros vs. Chile*" la Corte IDH señaló que la Convención en su artículo 13.1, ampara no solo el derecho de toda persona a recibir información sino que también implica la obligación positiva del Estado de suministrarla, al tiempo que reconoció el "*principio de máxima divulgación*", que implica la presunción de que toda información proveniente del Estado es accesible, sujeto a un sistema restringido de excepciones (Corte IDH, Caso "*Claude Reyes y otros c/Chile*", del 19/IX/2006, Serie C, 151).

IV.2. Continuando el análisis normativo que conforma el bloque de juridicidad en el que se encuentra inmerso el derecho de acceso a la información pública, corresponde remitirnos a las disposiciones de la Constitución de la Ciudad Autónoma de Buenos Aires.

El artículo 1° establece que la Ciudad "*organiza sus instituciones autónomas como democracia participativa y adopta para su gobierno la forma republicana*".

Por su parte, el artículo 12, inciso 2°, prevé que la Ciudad garantiza "[e]*l derecho a comunicarse, requerir, difundir y recibir información libremente y expresar sus opiniones e ideas, por cualquier medio y sin ningún tipo de censura*".

Finalmente, en lo que a la cuestión atañe, el artículo 16 dispone que "[t]*oda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos que conste en organismos públicos o en los privados destinados a proveer informes, a fin de conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga*".

IV.3. En el plano legal, la ley 104 establece que toda persona tiene derecho a solicitar y recibir información completa, veraz, adecuada y oportuna, de cualquier órgano perteneciente a la administración, tanto central como descentralizada, y de los demás entes y órganos que menciona (art. 1°), previendo una acción ante el fuero CAyT frente a la negativa a brindar la información de acceso público que hubiera

sido requerida (art. 12°).

Interesa remarcar que el art. 2º de la ley 104 prevé los principios de aplicación de la ley, según los cuales "[e]*l Derecho de Acceso a la Información Pública se interpretará conforme a la Constitución de la Nación, Constitución de la Ciudad Autónoma de Buenos Aires y a la Declaración Universal de los Derechos Humanos, al Pacto Internacional de Derechos Civiles y Políticos, a la Convención Americana sobre Derechos Humanos y a los instrumentos jurídicos internacionales sobre derechos humanos suscritos y ratificados por la República Argentina.*

Para la interpretación de esta ley se aplicarán los siguientes principios: 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".

A su vez, mediante el art. 3° enumera los sujetos obligados, entre los cuales se encuentran "[t]*odos los órganos pertenecientes a la administración central, descentralizada, entes autárquicos u organismos interjurisdiccionales integrados por la Ciudad Autónoma de Buenos Aires*" (inc. a).

En cuanto al alcance del derecho, el art. 4º estipula que "[d]*eberá proveerse la información contenida en documentos escritos, fotográficos, grabaciones, soporte magnético, digital o en cualquier otro formato, incluyendo bases de datos, acuerdos, directivas, reportes, estudios, oficios, proyectos de ley, disposiciones, resoluciones, providencias, expedientes, informes, actas, circulares, contratos, convenios, estadísticas, instructivos, dictámenes, boletines o cualquier otra información registrada en cualquier fecha, forma y soporte; que haya sido creada u obtenida por el órgano requerido, y que se encuentre en su posesión y bajo su control*".

Asimismo, el art. 5º prevé que "[l]*a información debe ser brindada en el estado en que se encuentre al momento de efectuarse la solicitud. En el caso de no poseer la información requerida, el órgano consultado tiene la obligación de informar los motivos por los cuales no la posee*".

Luego, el art. 6° establece que "[l]*os sujetos obligados podrán exceptuarse de proveer la información solicitada cuando se configure alguno de los siguientes supuestos:*

a) Que afecte la intimidad de las personas o se trate de información

referida a datos sensibles en concordancia con la Ley de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires. Esta excepción no será aplicable cuando existan mecanismos técnicos para disociar la información sensible o bien no sea necesario el consentimiento o cuando se cuente con el consentimiento expreso de la/s persona/s a las que se refiere la información solicitada;

b) Que sea información protegida por la legislación vigente en materia de derechos de autor, propiedad intelectual, secreto profesional, secreto industrial o comercial que pudieren afectar el nivel de competitividad o lesionar intereses del sujeto obligado;

c) Información cuya publicidad pudiera revelar la estrategia a adoptarse en la defensa o tramitación de una causa judicial en la cual el sujeto obligado sea parte, o divulgare las técnicas o procedimientos de investigación. Esta excepción no será aplicable cuando existan mecanismos técnicos para disociar la estrategia de defensa, técnicas o procedimientos de investigación del resto de las actuaciones;

d) Que se trate de información de terceros que la administración hubiera obtenido en carácter confidencial, que pudiera poner en peligro el correcto funcionamiento del sistema financiero, bancario o estadístico, o que esté protegida por el secreto bancario o fiscal o estadístico;

e) Que la divulgación pudiera ocasionar de manera verosímil un riesgo a la seguridad pública;

f) Información de carácter judicial cuya divulgación estuviere vedada por compromisos internacionales asumidos por la Ciudad Autónoma de Buenos Aires;

g) Información contenida en notas internas u opiniones producidas como parte del proceso previo a la toma de una decisión de autoridad pública que no formen parte de los expedientes…".

Seguidamente, se aclara que "[e]*n caso que exista un documento que contenga en forma parcial información cuyo acceso esté limitado en los términos del Artículo 6°, debe suministrarse el resto de la información solicitada*" (conf. art. 7º).

Finalmente, interesa recordar que "[l] *denegatoria de la información debe ser dispuesta por un/una funcionario/a de jerarquía equivalente o superior a Director General, en forma fundada. La denegatoria solo procede en aquellos casos en que la información no exista y cuando el funcionario no esté legalmente obligado a*

producirla o cuando se produzca alguna de las excepciones previstas en al Artículo 6° de la presente Ley, debiéndose exponer de manera detallada los elementos y las razones que la fundan" (conf. art. 13, ley 104, t.c. 2018).

IV.4. En otro orden de ideas, corresponde reseñar la normativa específica vinculada con la temática que aquí se ventila.

En primer término, la Constitución porteña garantiza en su art. 12 inc. 3 "[e]*l derecho a la privacidad, intimidad y confidencialidad como parte inviolable de la dignidad humana*".

A su vez, en su art. 34 establece que "[l]*a seguridad pública es un deber propio e irrenunciable del Estado y es ofrecido con equidad a todos los habitantes.*

El servicio estará a cargo de una policía de seguridad dependiente del Poder Ejecutivo, cuya organización se ajusta a los siguientes principios:

El comportamiento del personal policial debe responder a las reglas éticas para funcionarios encargados de hacer cumplir la ley, establecidas por la Organización de las Naciones Unidas.

La jerarquización profesional y salarial de la función policial y la garantía de estabilidad y de estricto orden de méritos en los ascensos.

El Gobierno de la Ciudad coadyuva a la seguridad ciudadana desarrollando estrategias y políticas multidisciplinarias de prevención del delito y la violencia, diseñando y facilitando los canales de participación comunitaria".

En tal sentido, la ley 5688, publicada en el BOCBA 5030 del 21/XII/2016, "*establece las bases jurídicas e institucionales fundamentales del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires en lo referente a su composición, misión, función, organización, dirección, coordinación y funcionamiento, así como las bases jurídicas e institucionales para la formulación, implementación y control de las políticas y estrategias de seguridad pública*" (conf. art. 1º).

El art. 2º define "*seguridad pública*" como "*la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establecen la Constitución Nacional y la Constitución de la Ciudad Autónoma de Buenos Aires*".

A su vez, mediante el art. 3° la ley 5688 establece que la seguridad pública "*implica la acción coordinada y la interacción permanente entre las personas y las instituciones del sistema democrático, representativo y republicano, particularmente, los organismos componentes del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires*" y mediante el art. 4º se afirma que la seguridad pública "*es deber propio e irrenunciable del Estado de la Ciudad Autónoma de Buenos Aires, que debe arbitrar los medios para salvaguardar la libertad, la integridad y derechos de las personas, así como preservar el orden público, implementando políticas públicas tendientes a asegurar la convivencia y fortalecer la cohesión social, dentro del estado de derecho, posibilitando el goce y pleno ejercicio, por parte de las personas, de las libertades, derechos y garantías constitucionalmente consagrados*".

Asimismo, mediante su art. 15, la Legislatura porteña adhirió a la ley nacional 24.059, de Seguridad Interior y su decreto reglamentario 1.273/PEN/92 y declaró que participa e integra en todas las instancias creadas por la ley nacional 25.520 de Inteligencia Nacional.

Mediante el art. 483 de la ley 5688 se expresó que "[e]*l acceso a toda información obtenida como consecuencia de las grabaciones se restringe a aquellos funcionarios que el Poder Ejecutivo individualmente determine, por razón de su función específica. Se prohíbe la cesión o copia de las imágenes salvo en los supuestos previstos en el presente Libro o en aquellos que se dispongan por vía reglamentaria o en el propio interés del titular*".

Luego, el art. 484 de la ley 5688 dispuso que "[c]*ualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones debe observar la debida reserva, confidencialidad y sigilo…*" y que "[l]*as grabaciones son destruidas una vez transcurridos sesenta (60) días corridos desde su captación* [salvo] *las que estén relacionadas con infracciones penales o administrativas en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto*".

Mediante el art. 474, la ley 5688 creó el SISTEMA PÚBLICO INTEGRAL DE VIDEO VIGILANCIA de la CABA. Luego, el art. 475 establece que dicho título "*regula la utilización por parte del Poder Ejecutivo de los sistemas de video vigilancia destinados*

a grabar imágenes en lugares públicos y a los que se refieren los artículos 485 y 486, estableciendo específicamente el posterior tratamiento de tales imágenes y el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente en las sucesivas fases de grabación y uso de las imágenes".

Seguidamente, el art. 476 prevé que "[l]*a 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.*

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".

A nivel nacional, cabe destacar que mediante la ley 13.482, publicada en el BO 16185 del 20/X/1948, se creó el REGISTRO NACIONAL DE LAS PERSONAS (RENAPER), dependiente del MINISTERIO DEL INTERIOR "*con la misión de registrar y certificar la identidad de todas las personas de existencia visible de nacionalidad argentina o que se hallen en jurisdicción argentina o se domicilien en ella, exceptuándose al personal diplomático extranjero, de acuerdo con las normas y convenios internacionales de reciprocidad*" (conf. art. 1º).

Asimismo, a dicho organismo se le asignaron las facultades de: "*a) Identificar e inscribir a todas las personas comprendidas en la enumeración del artículo 1, registrando los elementos que las indiquen y manteniéndolos actualizados b) Clasificarlos de modo que puedan ser utilizados: 1. - Por las autoridades públicas, a fines militares, electorales y demás que se fijen en la reglamentación 2. - Por los particulares c) Expedir los informes, certificados o testimonios previstos por esta ley d) Realizar, en coordinación con las autoridades pertinentes, las actividades estadísticas*

para asegurar el censo permanente de las personas" (conf. art. 2º).

Por su parte, la ley 24.059 a la que adhirió la Ciudad, publicada en el BO 27307 del 17/I/1992, establece las bases jurídicas, orgánicas y funcionales del sistema de planificación, coordinación, control y apoyo del esfuerzo nacional de policía tendiente a garantizar la seguridad interior (conf. art. 1º). A su vez, define "*seguridad interior*" como "*la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional*" (conf. art. 2º) y afirma que aquella "*implica el empleo de los elementos humanos y materiales de todas las fuerzas policiales y de seguridad de la Nación a fin de alcanzar los objetivos del artículo 2º*" (conf. art. 3º).

Por su parte, el decreto 346/PEN/09, publicado en el BO 31639 del 23/IV/2009, aprobó la creación del SISTEMA DE CONSULTA NACIONAL DE REBELDÍAS Y CAPTURAS (CONARC) "*con el objeto de brindar información inmediata a través del desarrollo de un sistema punto a punto, de manera actualizada de la totalidad de los autos de rebeldía, capturas, averiguación de paradero y comparendos que posee la Dirección Nacional del Registro Nacional de Reincidencia*" (conf. art. 1º).

Se estableció que el órgano de ejecución del Sistema es la DIRECCIÓN NACIONAL DEL REGISTRO NACIONAL DE REINCIDENCIA dependiente de la SUBSECRETARIA DE ASUNTOS REGISTRALES de la SECRETARÍA DE ASUNTOS REGISTRALES del MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS (conf. art. 2º), y se estableció que dicho organismo "*determinará la forma de acceso a la información, resguardando la protección de datos a través de las medidas de seguridad pertinentes, conforme lo dispuesto en el marco de la Ley Nº 22.117 y su reglamentación*" (conf. art. 3º).

Posteriormente, mediante el decreto 1766/PEN/11, publicado en el BO 32272 del 08/XI/2011, creó el SISTEMA FEDERAL DE IDENTIFICACIÓN BIOMÉTRICA PARA LA SEGURIDAD (SIBIOS) "*que tendrá por objeto prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales, a los fines de contribuir a la comprobación idónea y oportuna en materia de identificación de personas y rastros, en procura de optimizar la investigación científica de delitos y el*

apoyo a la función preventiva de seguridad" (conf. art. 1º).

En lo que aquí interesa, mediante la resolución 398/MJYSGC/19, publicada en el BOCBA 5604 del 25/IV/2019, se aprobó la implementación en el ámbito de la CABA, el SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS, cuya operación y funcionamiento quedará sujeto a lo dispuesto en el anexo que integra la norma (conf. art. 1º). Asimismo, se facultó a la SECRETARÍA DE JUSTICIA Y SEGURIDAD del MINISTERIO DE JUSTICIA Y SEGURIDAD a dictar las normas complementarias, operativas y aclaratorias que resulten necesarias y pertinentes para su efectiva implementación (conf. art. 2º). A la vez, se invitó a la DEFENSORÍA DEL PUEBLO de la CABA a auditar el funcionamiento del sistema, a cuyo fin se instituyó a la SECRETARÍA DE JUSTICIA Y SEGURIDAD del MINISTERIO DE JUSTICIA Y SEGURIDAD a gestionar la suscripción del pertinente convenio entre ambos (conf. art. 3º).

Luego, en dicho Anexo se estableció que "[e]*l Sistema de Reconocimiento Facial de Prófugos operará por intermedio del Sistema Público Integral de Video Vigilancia de la Ciudad Autónoma de Buenos Aires (Libro VII, artículos 474 y ss. de la Ley N° 5.688 [texto consolidado por Ley N° 6.017]) con arreglo a los ejes fundamentales y principios rectores plasmados en dicha ley*" (conf. art. 1º, anexo resolución 398/MJYSGC/19).

Asimismo, dispone que "[e]*l 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*" (conf. art. 2º, anexo resolución 398/MJYSGC/19).

Luego, el art. 3º del anexo de la resolución 398/MJYSGC/19 prevé que "[e]*l Sistema de Reconocimiento Facial de Prófugos se integra con la totalidad de los registros incorporados en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC) y con los datos biométricos consultados del Registro Nacional de las Personas (RENAPER), debiendo corresponder estos últimos única y exclusivamente a personas que registren orden judicial de restricción de la libertad registradas en la*

base del CONARC. Este requerimiento deberá ser dirigido a la Secretaría de Justicia y Seguridad".

Finalmente, el art. 4º estableció que "[e]*l 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*".

V. Sentado el marco normativo, corresponde analizar las respuestas brindadas por el GCBA a los interrogantes planteados y establecer si las denegatorias encuentran justificación en la inexistencia de la información en cuestión (art. 13 de la ley 5784) o en alguna de las excepciones legalmente establecidas (art. 6º de la ley 5784).

Ello, con relación a la información solicitada en las preguntas identificadas en el considerando **III**, esto es: 10, 13, 20, 26, 44, 45, 47, 52, 53, 58, 61, 62, 67, 76 y 77.

V.1. Pregunta 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?*

Respecto de esta pregunta, el GCBA emitió la nota NO-2019-33745359-GCABA-DGEYTI, del 30/X/2019, acompañada en soporte digital reservado por Secretaría a fs. 93, en el archivo titulado "*4.- NO-2019-33745359-GCABA-DGEYTI*". Allí, la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA indicó que: "[e]*l Centro de Monitoreo Urbano (CMU) cuenta con un Protocolo de actuación sobre el Procedimiento en caso de alerta arrojada por el `Sistema de Reconocimiento Facial de Prófugos´. Asimismo cuenta con un Convenio de Confidencialidad utilizado para la totalidad del personal del Centro de Monitoreo Urbano de acuerdo a lo normado en el artículo 483 de la Ley Nº 5.688/16. Por último, el CMU implementó la gestión de seguimiento de calidad respecto al sistema de reconocimiento facial de prófugos*". En tal sentido, acompañó el modelo de declaración jurada de confidencialidad al que aludió, que se encuentra en el archivo denominado "*5.-Declaración+Jurada+de+Confidencialidad+Personal+Civil-Policial+2019+(SIP)*" grabado en el soporte digital reservado a fs. 93. En dicho modelo de declaración jurada

de confidencialidad, en su punto 7, se indica que quien la suscribe "[c]*onoce el Protocolo de Actuación respecto al procedimiento de intervención en caso de alerta del Sistema de Reconocimiento Facial de Prófugos*". Además, informó que "[l]*a información desde que es capturada hasta que llega al CMU viaja encriptada mediante aplicabilidad de protocolo 3DES*" (fs. 104/118).

Sin embargo, la parte actora esgrimió que "[s]*i bien la Administración manifiesta tener un Protocolo de Actuación sobre el Procedimiento en caso de Alerta Arrojada por el SREP, lo cierto es que la pregunta estaba destinada a comprender de qué manera la administración mantiene segura la información capturada hasta su destino final en el CMU*" y que "*si bien la Administración señala que este Protocolo de Actuación existiría, la misma no lo ha acompañado*" (v. fs. 94 vta./95 y 120/125 vta.). Asimismo, planteó que "*la información solicitada es necesaria a los fines de poder determinar si ha existido o existe una Evaluación de Impacto de la Privacidad (EIP) respecto del sistema de reconocimiento facial*" (fs. 7 vta.).

Ahora bien, examinada la respuesta del GCBA, resulta claro que la información suministrada al peticionante es insuficiente. En efecto, la requirente consultó por los protocolos destinados a mantener la privacidad de la información recopilada desde su captura hasta su procesamiento, cuestión sobre la que el legislador porteño se preocupó, conforme surge de los artículos 483 y 484 de la ley 5688.

Por otra parte, el GCBA omitió acompañar el *Protocolo de Actuación sobre el Procedimiento en caso de Alerta Arrojada por el SREP* que, a su entender, tendría vinculación con las medidas de privacidad de las imágenes sobre las cuáles fue requerido informar.

De lo expuesto hasta aquí, se observa que la información suministrada resulta parcial e insuficiente, sin que el GCBA hubiera esgrimido alguna de las causales previstas en el art. 6º de la ley 104 para exceptuarse de proveer la información solicitada o se hubiera amprado en la inexistencia de la información en cuestión (art. 13 de la ley 104).

Por lo tanto, corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la pregunta 10.

V.2. Pregunta 13: *¿Qué técnica de borrado es utilizada? ¿Cómo se audita y de qué manera se asegura que las imágenes son efectivamente eliminadas?*

Respecto de esta pregunta, el GCBA se limitó a responder que "[l]*a auditoría del funcionamiento del Sistema de Reconocimiento Facial de Prófugos es llevada a cabo por la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires*" (nota NO-2019-25581723-GCABA-DGEYTI, del 15/VIII/2019, cuya copia luce a fs. 20/22 vta. -cuya autenticidad no fue desconocida expresamente por la contraparte-). Luego, mediante la nota NO-2019-33745359-GCABA-DGEYTI antes citada, la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93- indicó que: "[l]*a auditoría del funcionamiento del Sistema de Reconocimiento Facial de Prófugos es llevada a cabo por la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires. El sistema de referencia no almacena imágenes a excepción de las alertas correspondiente a aquellas personas buscadas por la justicia. Conforme a lo enunciado, las imágenes que no devienen en una alerta positiva son automáticamente descartadas del proceso de almacenamiento del sistema*". Ello fue reiterado en los siguientes términos "*el SRFP no almacena imágenes de las lecturas realizadas, excepto sea una lectura positiva. Es decir, que la persona se encuentra en la base de datos del CONARC impartida por la justicia. En estos casos, estas imágenes reciben el mismo tratamiento que el estipulados en la Ley original N. 2602/08 abrogada por la ley 5688/16*" (fs. 104/118 vta.).

Con relación a ello, la parte actora manifestó que "*la administración ha obviado totalmente contestar la pregunta acerca de la técnica de borrado que debería ser utilizada al eliminar la información recopilada por las cámaras*" y que tampoco "*ha determinado de qué manera se debería llevar a cabo la auditoría del sistema. La administración se limitó a repetir información que ya había provisto anteriormente*", agregando que a su entender "*la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires es el ente que debería auditar el sistema pero la pregunta iba dirigida a otra cuestión*" (v. fs. 95). En tal sentido, también señaló que la Administración no respondió "*acerca de qué manera es realizada la auditoría del borrado de las imágenes, ni tampoco cuál es la técnica de borrado utilizada*" (fs. 7 vta.). Asimismo, dijo "[l]*a pregunta nuevamente no ha sido contestada. No se ha hecho referencia alguna a la técnica de borrado de las imágenes. Es evidente que si las imágenes son trasladas desde la captura de la imagen en las cámaras al CMU que aunque sea*

provisoriamente, dichas imágenes deben ser almacenadas en algún elemento físico. Existen distintas técnicas de borrados tales como la desmagnetización, destrucción física, sobre-escritura,, métodos de borrado provistos por el mismo sistema y que pueden ser altamente inseguros, etc." (fs. 120/125 vta.).

A fin de evaluar este punto, cabe comenzar por señalar que esta pregunta contenía tres partes: *(a) ¿Qué técnica de borrado es utilizada?; (b) ¿Cómo se audita dicho borrado?; y (c) ¿De qué manera se asegura que las imágenes son efectivamente eliminadas?*.

Respecto de la primera parte de la pregunta, no se observa respuesta alguna por parte del GCBA.

Con relación a la segunda parte de la pregunta, el GCBA contestó que "[l]*a auditoría del funcionamiento del Sistema de Reconocimiento Facial de Prófugos es llevada a cabo por la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires*". Sin embargo, la pregunta no fue por el "*quién*" sino por el "*cómo*", es decir, por el mecanismo, el modo, la manera, la técnica. Respecto de esto nada informó el GCBA.

Finalmente, en cuanto a la tercera parte de la pregunta, esto es, de qué manera se asegura que las imágenes son efectivamente eliminadas, nada informó el GCBA. En efecto, al decir que "[e]*l sistema de referencia no almacena imágenes a excepción de las alertas correspondiente a aquellas personas buscadas por la justicia*" y que "*las imágenes que no devienen en una alerta positiva son automáticamente descartadas del proceso de almacenamiento del sistema*", eludió la respuesta específica que le estaba siendo requerida.

Por lo tanto, no habiendo esgrimido alguna de las causales previstas en el art. 6º de la ley 104 para exceptuarse de proveer la información solicitada y sin que se hubiera amprado en la inexistencia de la misma (art. 13 de la ley 104), corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la pregunta 13.

V.3. Pregunta 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?***

Con relación a esta pregunta, si bien en un principio el GCBA mantuvo silencio, luego sostuvo que "[a] *través de la Nota NO-2019-36772362-GCABA-SIOOU*

el Estado manifestó `[…] que por medio del presente se informa que se han ingresado un total de 43 altas al Sistema de Reconocimiento Facial de Prófugos por requerimiento judicial […]´" (fs. 104/118 vta.).

En tal sentido, la parte actora señaló que "[e]*sta pregunta ha sido directamente obviada por el GCBA*" (fs. 95), siendo necesaria "*para evaluar la seguridad del sistema*" (fs. 7 vta.). Luego, ante la respuesta de fs. 104/118 vta., afirmó: "[m]*i parte no tiene manera de determinar si dicha respuesta está orientada a esta pregunta pero en el caso que así sea debo destacar que en ningún momento se aclara si dichas altas corresponden a altas en la Base de Datos del CONARC o si directamente utilizaron datos provistos por estos `requerimientos judiciales´ para hacer una especie de alta manual en el SRFP*" (fs. 120/125 vta.).

En este sentido, cabe señalar que asiste razón a la actora en el sentido de que la respuesta brindada por el GCBA luce por demás imprecisa, ya que omite informar cuántas de las imágenes ingresadas al sistema no estaban registradas en el CONARC. Tampoco se justifica la referida imprecisión en la presunta inexistencia de dicha información (conf. art. 13, ley 104).

Por lo tanto, corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la pregunta 20.

V.4. Pregunta 26: *¿A qué requerimiento se refiere la última parte del art. 3* [del anexo de la resolución 398/MJYSG/19]*? ¿Por qué este requerimiento tiene que estar dirigido a la Secretaría de Justicia y Seguridad?*

En esta pregunta se está aludiendo al art. 3º del Anexo de la resolución 398, según el cual "[e]*l sistema de Reconocimiento Facial de Prófugos se integra con la totalidad de los registros incorporados en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC) y con los datos biométricos consultados del Registro Nacional de las Personas (RENAPER), debiendo corresponder estos últimos única y exclusivamente a personas que registren orden judicial de restricción de la libertad registradas en la base del CONARC. Este requerimiento deberá ser dirigido a la Secretaría de Justicia y Seguridad*".

Según indicó la parte actora, sus dudas recaen en la última oración del párrafo transcripto (v. fs. 95 vta.). Asimismo, señaló que dicha información "*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" (fs. 7 vta.).

De la totalidad de constancias acompañadas en autos, es dable advertir que esta pregunta no ha sido respondida por el GCBA, sin que hubiera esgrimido alguna de las causales previstas en los arts. 6º y 13 de la ley 104.

Por lo tanto, corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la pregunta 26.

V.5. 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 protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos? y ¿Cómo se audita su correcta destrucción?*

Respecto de esta pregunta, el GCBA en una primera oportunidad respondió: "[t]*eléfono institucional (POC)*" (nota NO-2019-25581723-GCABA-DGEYTI, del 15/VIII/2019, cuya copia luce a fs. 20/22 vta.). Posteriormente, dicha respuesta fue ampliada en los siguientes términos, que surgen de la nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-. Allí, con relación a la primera parte (¿*En qué tipo de aparatos reciben las alertas generadas por el sistema los agentes de la Policía*?) señaló: "[t]*eléfono institucional (POC), mediante el cual el personal policial efectúa comunicaciones respecto a necesidades operativas. Las alertas son recibidas únicamente en los teléfonos asignados a los efectivos abocados a dicha tarea. La tecnología de estos dispositivos son Smartphone con tecnología 4G, sistema Androide, marca Samsung*". Asimismo, sostuvo "*los dispositivos utilizados utilizan un Smartphone con tecnología 4G; sistema operativo Android de la marca Samsung -en sus diferentes modelos-, están interconectados a la red del MJYS a través de un APN provista por la firma Telefónica de Argentina S.A. Estos equipos tienen instalado el sistema MDA y Airwatch, lo que hace que el mismo sea un quiosco y no tenga ningún tipo de conexión hacia otras redes de datos que no sea lo provisto por este Ministerio. Una vez tratadas las alertas positivas, estas se eliminan del equipo de forma automática*" (fs. 104/118 vta.).

Respecto de la segunda parte de la pregunta (*¿En qué momentos los agentes destruyen aquellos archivos que le fueron enviados a esos aparatos?*) indicó: "[l]*os teléfonos institucionales no almacenan eventos*".

Finalmente, respecto de la tercera parte de la pregunta (*¿Qué sistema o protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos y como se audita su correcta destrucción?*) mantuvo silencio.

Al respecto, la parte actora expresó que "[e]*l GCBA no explica qué 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.*" (fs. 7 vta./8). Además, dijo que "[e]*l GCBA no indica qué tipo de aparatos se utiliza. No especifica sistema operativo, ni modelo del aparto ni a qué red se conectan para el envío de la información. El hecho de que reciban eventos implica que efectivamente los reciban por lo que se deben guardar en la memoria del teléfono*"; al tiempo que manifestó que "[d]*irectamente omiten establecer el protocolo de seguridad que se debiera seguir para la protección de los datos generados*". Además, señaló que "[t]*ampoco hicieron referencia alguna a si existe auditoría de esos aparatos para la eliminación de los eventos*" (fs. 95 vta./96). Finalmente, sostuvo "[e]*l estado sigue sin contestar si se realiza una auditoría de estos aparatos para determinar si la información es efectivamente borrada*" (fs. 120/125 vta.).

Ahora bien, la presente pregunta puede dividirse en cuatro partes, a saber: *a) ¿En qué tipo de aparatos reciben las alertas generadas por el sistema los agentes de la Policía?; b) ¿En qué momentos los agentes destruyen aquellos archivos que le fueron enviados a esos aparatos?; c) ¿Qué sistema o protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos?;* y *d) ¿Cómo se audita su correcta destrucción?*

En tal sentido, estimo que la primera parte de la pregunta fue contestada satisfactoriamente, en tanto el GCBA señaló que es recibida en el "[t]*eléfono institucional (POC)*" (fs. 20/22 vta.), a lo que agregó que se trata del "[t]*eléfono institucional (POC), mediante el cual el personal policial efectúa comunicaciones respecto a necesidades operativas. Las alertas son recibidas únicamente en los teléfonos asignados a los efectivos abocados a dicha tarea. La tecnología de estos dispositivos son Smartphone con tecnología 4G, sistema Androide, marca Samsung*"

(nota NO-2019-33745359-GCABA-DGEYTI, en soporte digital reservado por Secretaría a fs. 93) y que "*los dispositivos utilizados utilizan un Smartphone con tecnología 4G; sistema operativo Android de la marca Samsung -en sus diferentes modelos-, están interconectados a la red del MJYS a través de un APN provista por la firma Telefónica de Argentina S.A. Estos equipos tienen instalado el sistema MDA y Airwatch, lo que hace que el mismo sea un quiosco y no tenga ningún tipo de conexión hacia otras redes de datos que no sea lo provisto por este Ministerio. Una vez tratadas las alertas positivas, estas se eliminan del equipo de forma automática*" (fs. 104/118 vta.).

En efecto, sin perjuicio de la manifestación realizada por la parte actora en el sentido de que "[e]*l GCBA no indica qué tipo de aparatos se utiliza. No especifica sistema operativo, ni modelo del aparto ni a qué red se conectan para el envío de la información. El hecho de que reciban eventos implica que efectivamente los reciban por lo que se deben guardar en la memoria del teléfono*" (fs. 95 vta./96) no parece atendible. Ello, en tanto el sistema operativo sí fue informado (androide), así como el tipo de aparato también (*Smartphone con tecnología, marca Samsung*) y también la red a la que se conectan para el envío de información (*red del MJYS a través de un APN provista por la firma Telefónica de Argentina S.A*). En tal sentido, sin perjuicio de que la consulta original no incluía la necesidad de informar especificaciones técnicas sobre el aparato, sino que aludía meramente al tipo de aparato, se advierte que las inquietudes posteriormente manifestadas por la actora fueron efectivamente evacuadas. Desde este vértice, este Tribunal estima que dicha primera parte de la pregunta 44 fue adecuadamente respondida por el GCBA.

Con relación a la segunda parte de la pregunta, esto es, en qué momento los agentes destruyen aquellos archivos que le fueron enviados a esos aparatos, cabe recordar que el GCBA informó que "[l]*os teléfonos institucionales no almacenan eventos*". Ahora bien, este Tribunal comparte la afirmación vertida por la actora al decir que "[e]*l hecho de que reciban eventos implica que efectivamente los reciban por lo que se deben guardar en la memoria del teléfono*". Expresión que sugiere que la recepción de los "*eventos*" en el aparato es aquella que permite que los agentes accedan a su contenido y, en consecuencia, ello implica que la información sea o pueda ser almacenada al menos algún periodo mínimo de tiempo. En tal sentido, la afirmación de

que dichos teléfonos no almacenan "*eventos*" (expresión que -por cierto- introduce el GCBA al responder pero no necesariamente es equivalente a "*archivos*", término empleado por la parte actora al hacer la consulta) luce confusa. Si dicha información se autodestruye segundos más tarde de su recepción o si los agentes tienen la obligación de destruirla dentro de un periodo determinado, entre otros interrogantes que surgen a partir de la respuesta brindada por el GCBA, son cuestiones que merecen una respuesta más clara y concreta, demostrativa de su voluntad de dar pleno cumplimiento al requerimiento de información, conforme la buena fe (conf. art. 2º, segundo párrafo, ley 104). La respuesta, en los términos en que fue brindada, abre más interrogantes que certezas, y por lo tanto, no puede considerarse satisfactoria en el marco del presente proceso.

Por último, respecto de las tercera y cuarta partes de la pregunta 44 (*¿Qué sistema o protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos?* y *¿Cómo se audita su correcta destrucción?*), cabe notar que el GCBA mantuvo silencio y, en consecuencia, tampoco dio satisfacción al requerimiento efectuado.

Por lo tanto, corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en las segunda, tercera y cuarta partes de la pregunta 44 –respecto de las cuales no invocó ni fundó causal alguna contemplada en la ley 104- y dar por contestada la primera parte de dicha pregunta.

V.6. Pregunta 45: *¿A través de qué sistema les llegan las alertas generada a los Policías? ¿Qué información les es remitida?*

Respecto de esta pregunta, el GCBA respondió: "[a] *través de una APK específica de desarrollo propio. Información respecto a la captura de la persona proporcionada por el CONARC*" (nota NO-2019-25581723-GCABA-DGEYTI, del 15/VIII/2019, cuya copia luce a fs. 20/22 vta.). Además, señaló "*los teléfonos institucionales provistos reciben alertas a través de una ampliación donde enuncia; la foto de la persona prófuga de la justicia, número de cámara de video que la detectó y toda aquella información de la causa judicial extraída del CONARC. La accesibilidad a esta aplicación únicamente es obtenida por personal policial asignados a estos operativos dentro de la red del MJTS*" (fs. 104/118 vta.). Luego, añadió: "[l]*as alertas llegan a los efectivos asignados a dicha función mediante una APP*

(aplicación) específica de desarrollo propio, la cual posee normas de seguridad y uso (control de logging, y marca de agua en usuarios)" (nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-).

Al respecto, la parte actora sostuvo que el GCBA "[n]*o indica que información es efectivamente remitida a los agentes de la policía y tampoco explica qué sistema es utilizado para la remisión de esa información. No explica a qué se refiere con `APK'*" (fs. 7 vta./8). Asimismo, refirió que "[e]*l hecho de que se limiten a comentar que el sistema es de desarrollo propio es nuevamente de una absoluta necedad que no hace al objeto de la pregunta*". Además, plantea que "[s]*i efectivamente es de desarrollo propio, cuál es su nombre, de qué manera se puede tener acceso a él, cuáles son las normas de seguridad y uso que le aplican*" y agrega "*la Administración no contesta nada acerca de la información que le es remitida a los policías abocados a este SRFP*" (fs. 96/96 vta.).

Respecto de esta pregunta 45, también cabe dividirla en dos partes: la primera, sobre el sistema a través del cual les llegan las alertas generada a los Policías, y la segunda, acerca de la información que les es remitida a dichos policías.

En cuanto a la primera parte de la pregunta, el GCBA informó que "[l]*as alertas llegan a los efectivos asignados a dicha función mediante una APP (aplicación) específica de desarrollo propio, la cual posee normas de seguridad y uso (control de logging, y marca de agua en usuarios)*". En tal sentido, cabe notar que dicha respuesta aparece como insuficiente, en tanto la pregunta estaba expresada en términos amplios (*¿qué sistema?*) lo que evidencia una necesidad de acceder a toda la información disponible sobre dicho sistema, más allá de saber que es de desarrollo propio. Además, si posee normas de seguridad y uso como lo afirma la demandada, resulta necesario que se especifiquen dichas medidas, lo que no se satisface aludiendo meramente al control de logging y a la marca de agua en usuarios. En caso de que esas fueran las únicas medidas de seguridad del sistema, ello deberá ser informado, así como "*cuál es su nombre, de qué manera se puede tener acceso a él*" (fs. 96/96 vta.).

Con relación a la segunda parte de la pregunta, sobre la información que les es remitida a dichos policías, el GCBA refirió que se trata de "[i]*nformación*

respecto a la captura de la persona proporcionada por el CONARC". En tal sentido, es dable advertir que dicha respuesta luce incompleta y tautológica, en tanto va de suyo que se trata de información respecto de la captura de la persona aportada por el CONARC, de acuerdo con el sistema regulado por la resolución 398/MJYGC/19. En consecuencia, es dable considerar que dicha respuesta puede ser fortalecida por el GCBA a fin de dar satisfacción completa al requerimiento de información de autos.

Por lo tanto, corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la pregunta 45 –sobre la cual no justificó su negativa en los términos de los arts. 6º y 13 de la ley 104-.

V.7. Pregunta 47: *¿cuántos agentes reciben esta información?*

A esta pregunta, se ha contestado "[e]*l personal abocado por turno al servicio específico*" (nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-).

Al respecto, la parte actora alegó que "*la pregunta hacía referencia a cuántos agentes de la policía se le envía la información de las alertas*" (fs. 96 vta.) y que "*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´*" (fs. 7 vta.).

En este punto, cabe notar que la respuesta brindada por el GCBA ostenta una imprecisión injustificada. Es que, por un lado, omite informar un número -aunque sea aproximado- del personal que recibe dicha información, y por el otro, tampoco brinda una explicación que permita conocer las razones por las cuales estaría imposibilitado de proporcionar mayor precisión a la consulta realizada. Aquella imprecisión y falta de fundamentación suficiente de la misma obligan a este Tribunal a condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la pregunta 47, sin que sea posible tener por justificada la reticencia en alguna de las causales previstas en la ley 104 (en especial, arts. 6º y 13).

V.8. Pregunta 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 1068 – E/2016.

Sobre esta pregunta, el GCBA contestó que "[e]*l MJyS no es órgano competente para conceptuar o definir los delitos graves*" (nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-).

Sobre el punto, la parte actora manifestó "[p]*or supuesto que el MJyS no es órgano para conceptuar o definir qué es un delito grave. Precisamente por esa razón nos remitimos a la Resolución 1068 – E/2016 que conceptualiza dicha definición en el marco del Registro Nacional de Reincidencia que creara el CONARC*". Asimismo, señaló que "*el MJyS es el único que puede determinar cuántas personas han sido detenidas con causa en una alerta levantada por el SRFP y que a su vez nos pueda decir cuántas de ellas no eran buscadas por un `delito grave´ en los términos de la resolución mencionada*" (fs. 96 vta.). A su vez, la actora señaló que "[c]*onforme lo expuso el Relato*[r] *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 delimita*[dor] *resulta imperioso a los fines de determinar el universo de personas que conforman la lista/registro que posee el sistema*" (fs. 8).

Sobre este punto, cabe notar que la actora se remitió en la pregunta a la definición de "*delito grave*" que brinda la resolución 1068 – E/2016, publicada en el BO 33504 del 15/XI/2016. En tal sentido, el anexo de dicha resolución establece que "*a los fines de la implementación del Sistema "Los más buscados" se considerarán delitos graves aquellos previstos en el Código Penal de la Nación, Libro Segundo, Título I (Delitos contra las Personas); Título III (Delitos Contra la Integridad Sexual); Título IV (Delitos Contra el Estado Civil); Título V (Delitos Contra la Libertad); Título VII (Delitos Contra la Seguridad Pública); Título VIII (Delitos Contra el Orden Público), Título IX (Delitos Contra la Seguridad de la Nación); Título X (Delitos Contra la Poderes Públicos y el Orden Constitucional); Título XI (Delitos Contra la Administración Pública) y Título XIII (Delitos Contra el Orden Económico y Financiero).*

Asimismo, a los fines de su difusión a través del Sistema "Los más

buscados", se considerarán también delitos graves aquellos contenidos en las Leyes Nros. 22.415, 23.737 y 24.769.

En la totalidad de los casos, los delitos imputados deberán tener prevista una pena privativa de libertad cuyo mínimo sea superior a los tres (3) años de prisión.

Podrá igualmente ser incluido en el Sistema "Los más buscados", aquel caso que no cumpla con los requisitos señalados pero que por circunstancias especiales ponderadas por el magistrado solicitante se aconseje su difusión" (conf. art. 1º, anexo, resolución 1068 – E/2016).

Es decir que la pregunta debía completarse con la definición transcripta, sin que pueda ser alegado eficientemente para eludir su respuesta que "[e]*l MJyS no es órgano competente para conceptuar o definir los delitos graves*", como lo hizo la demandada. Tal afirmación no constituye justificación suficiente en los términos de lo dispuesto en los arts. 6º y 13 de la ley 104.

En consecuencia, a criterio de este Tribunal, el interrogante planteado por la actora subsiste en virtud de la respuesta brindada por el GCBA, que parece evadir su deber de suministrar la información requerida, violando así el principio de buena aplicable (conf. art. 2º, segundo párrafo, ley 104).

Por lo expuesto, corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la pregunta 52.

V.9. Pregunta 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"?***

Con relación a esta pregunta, el GCBA informó que "[a] *la actualidad, 1648 personas han sido identificadas y puestas a disposición de la justicia*" (nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-).

Al respecto, la parte actora señaló que "[l]*a Administración se limita a dar información ya provista*", remitiéndose a "*los mismos argumentos señalados en la pregunta anterior* [pregunta 52]" (fs. 96 vta./97). Respecto de esta pregunta, la parte actora también indicó que "[c]*onforme lo expuso el Relato*[r] *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 delimita[dor] *resulta imperioso a los fines de determinar el universo de personas que conforman la lista/registro que posee el sistema*" (fs. 8).

Al respecto, cabe notar que la respuesta brindada por el GCBA no da plena satisfacción a lo requerido, en tanto si bien informó que "[a] *la actualidad, 1648 personas han sido identificadas y puestas a disposición de la justicia*", omitió especificar cuántas de dichas personas estaban siendo buscadas en virtud de un delito grave, que era precisamente la información solicitada. Tal comportamiento impide tener por configurado alguno de los supuestos previstos en los arts. 6º y 13 de la ley 104.

Por lo expuesto, corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la pregunta 53.

V.10. Pregunta 58: ***Para el caso de que la empresa*** **[DANAIDE S.A., a quien se adjudicó directamente el contrato administrativo tendiente a desarrollar el SRFP]** ***entre en concurso, quiebra o cualquier otra forma reglamentaria dc 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?***

Al respecto, el GCBA nada ha dicho, y así lo puso de resalto la parte actora a fs. 97. Además, esta señaló que "*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 firm*[a] *deje de existir*", a la vez que "*se necesita a efectos de evaluar la posible ocurrencia de hechos contrarios a lo dispuesto por l*[a] *Ley de Compras y Contrataciones de la Ciudad*" (fs. 8).

Atento que el GCBA omitió brindar respuesta alguna al interrogante planteado en la pregunta 58 sin brindar justificación basada en alguna de las causales previstas en los arts. 6º y 13 de la ley 104, corresponde condenarlo a brindar la información requerida en sede administrativa.

V.11. Pregunta 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?***

Respecto de esta pregunta, el GCBA en un primer momento respondió

que "[e]*sta información corresponde al desarrollo del producto y es un detalle que posee el copyright de la licencia del mismo, por lo cual no se posee acceso a esta información*" (nota NO-2019-25581723-GCABA-DGEYTI, del 15/VIII/2019, cuya copia luce a fs. 20/22 vta.). Asimismo, sostuvo "[d]*ependiendo de la calidad de las imágenes obtenidas del cruzamiento de la base de datos de CONARC con el RENAPER, se utiliza alguno de los métodos siguientes: holístico, locales o Geométricos. Como set de datos para calibrar y verificar el funcionamiento del sistema, se realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los casos los porcentajes de error exigidos*" (fs. 104/118 vta.). Luego, señaló que "[s]*e realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los casos los porcentajes de error exigidos*" (nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-).

Con relación a ello, la parte actora señaló que "[e]*l 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 otro lado, cuando nos referimos al 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, VS podrá determinarlo por su propia cuenta*" (fs. 7 vta./8). Asimismo, manifestó que "[e]*l estado confirma que utilizaron, distintos sujetos de prueba pero no aporta a la causa aquellos datos para poder evaluar la idoneidad de esos datos para su entrenamiento*" (fs. 120/125 vta.). Luego, señaló que "[e]*l objeto de esta pregunta no se encuentra destinado a saber información protegida por derechos de propiedad intelectual de la empresa*

adjudicataria" y que "[e]n *los sistemas de reconocimiento facial se suelen utilizar distintos métodos de detección de rostros* [que] *tienen nombres técnicos como holísticos, locales o geométricos*" y mencionó que "*otros ejemplos de métodos que son el Análisis de Componentes Principales (PCA-Principal Component Analysis), el Análisis Linear Discriminante (LDA – Linear Discriminant Analysis) o el Discriminante Linear de Fisher (FLD – Fisher Linear Discriminant)*" (fs. 97). A ello, agregó que dicha información "*no tiene por qué estar protegida por copyright ya que es información técnica del producto que no es original del que provee el servicios sino que es meramente descriptiva del método que utilizaría el mismo*" y que "*el set de datos utilizado para entrenar el producto tampoco debería ser información protegida por copyright ya que la misma debería haber sido entrenada con imágenes de ciudadanos. A no ser que el mismo haya sido entrenado con imágenes de ciudadanos de otros países, lo cual hablaría bastante de la eficiencia que es un sistema entrenado con imágenes de un país con una demografía distinta a la nuestra, pero que de igual no estaría protegida por el copyright*" (fs. 97 vta.).

De la pregunta bajo análisis, es posible extraer distintas partes. Una primera parte de la pregunta alude al método de detección de rostros utilizado por el SRFP. Luego, una segunda parte de la pregunta apunta al supuesto de que se hubieran utilizado redes neuronales para elaborar dicho sistema y pregunta por el modelo/arquitectura y el set de datos utilizado para entrenar el modelo.

En cuanto a la primera parte de la pregunta, es dable considerar que la respuesta brindada por el GCBA resulta insuficiente, en tanto se limitó a decir que dicha información "*corresponde al desarrollo del producto y es un detalle que posee el copyright de la licencia del mismo, por lo cual no se posee acceso a esta información*". Sin embargo, cabe destacar que si su negativa a brindar la información solicitada se ampara en alguno de los supuestos previstos en el art. 6º de la ley 104 (v.g. inciso e), su esfuerzo argumentativo debería haber sido mayor. En efecto, el art. 13 de la ley 104 indica en caso de que la denegatoria se fundara en alguno de dichos supuestos, se debe "*exponer de manera detallada los elementos y las razones que la fundan*", lo que en el caso no acontece.

En cuanto a la segunda parte de la pregunta 61, vinculada con la hipótesis de que se hubieran empleado redes neuronales para elaborar el SRFP y en tal

caso, cuál fue el modelo/arquitectura y el set de datos utilizado para entrenar el modelo, se observa que la respuesta del GCBA carece de precisión y completitud. En efecto, meramente indicó que "[s]*e realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los casos los porcentajes de error exigidos*", sin que dicha generalidad permita satisfacer una pregunta que ostenta un grado bastante más alto de precisión. En efecto, de la respuesta brindada es posible colegir que la respuesta fue escueta y, en consecuencia, podría ser ampliada para dar plena satisfacción al requerimiento del Observatorio peticionante, dentro de un marco de buena fe (conf. art. 2º, segunda parte, ley 104).

Por lo tanto, corresponde condenar al GCBA a suministrar la información requerida en la pregunta 61 formulada en sede administrativa por la parte actora.

V.12. Pregunta 62: *¿Qué datasets fueron utilizados para ese entrenamiento y qué organismo fue responsable?*

Aquí, el GCBA informó que "[p]*rimera parte ídem, resp. N° 61. El organismo responsable fue el Ministerio de Justicia y Seguridad*" (nota NO-2019-25581723-GCABA-DGEYTI, del 15/VIII/2019, cuya copia luce a fs. 20/22 vta. y nota NO-2019-33745359-GCABA-DGEYTI, ambas de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-). A ello, agregó que "[c]*omo set de datos para calibrar y verificar el funcionamiento del sistema, se realizaron pruebas de campo con diferentes sujetos de prueba, con diferentes características físicas, y en diferentes escenarios, verificando que se cumplan en todos los casos los porcentajes de error exigidos*" (fs. 104/118 vta.).

Por su parte, la actora se remitió a lo señalado respecto de la respuesta a la pregunta 61 (fs. 97 vta.) y señaló que "[l]*a administración no identifica cuál fue el dataset utilizado para el entrenamiento de este Sistema*" (fs. 120/125 vta.).

En este punto, se advierte que si bien la segunda parte de la pregunta (*¿qué organismo fue responsable del entrenamiento?*) fue contestada al mencionar al MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA, la primera parte *(¿qué datasets fueron utilizados en dicho entrenamiento?*) no lo fue por los mismos motivos que se

señalaron en el considerando precedente, al que cabe remitirse.

En consecuencia, corresponde condenar al GCBA a brindar la información requerida en sede administrativa por la parte actora en la primera parte de la pregunta 62.

V.13. Pregunta 67: *¿Se ha hecho una auditoría del software por un tercero independiente?*

Sobre este punto, el GCBA señaló "[c]*onforme la Resolución 398/2019, la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires es el organismo auditor*" (nota NO-2019-25581723-GCABA-DGEYTI, del 15/VIII/2019, cuya copia luce a fs. 20/22 vta.). Luego, insistió en que "[c]*onforme a la Resolución 398/2019, se invita a la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires a auditar el funcionamiento del Sistema de Reconocimiento Facial de Prófugos*" (nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-), y agregó que "*a cuyo fin se concluyeron reuniones informativas y demostrativas de procedimientos reales en el Centro de Monitoreo Urbano - Centro Operativo del SRFP*" y "*se remitió la información técnica requerida a la Defensoría del Pueblo* [acerca del] *funcionamiento técnico y operativo del SRFP*" (fs. 104/118 vta.).

Así las cosas, la parte actora señaló que "[l]*a pregunta estaba dirigida a 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*" (fs. 6 vta./7). Luego, agregó que "[l]*a Administración no contesta la pregunta la cual fue directamente esquivada*" y aclaró que lo que quiere saber es "*si se realizó una auditoría del sistema o no*" (fs. 97 vta.).

En este sentido, este Tribunal advierte que, efectivamente, la respuesta brindada por el GCBA no da satisfacción a la pregunta. Subsiste al respecto la duda original, acerca de si un tercero independiente realizó o no una auditoría del funcionamiento del SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS y, en su caso, qué resultados arrojó. La reticencia a informarlo no aparece fundada en alguno de los supuestos previstos en los arts. 6º y 13 de la ley 104.

En consecuencia, corresponde condenar al GCBA a brindar la

información requerida en sede administrativa respecto de la pregunta 67.

V.14. Pregunta 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): "[…] 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 […]"(EI 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. ¿Cómo y que procedimiento se 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/ 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?

Con respecto a esta pregunta, el GCBA contestó lo siguiente: "[a]*partados A/B/F: en los que se requiere se indique `que se quiso decir´ con: `detección de diferentes patrones de comportamiento´ y `cambios de condiciones ambientales´, y en qué consisten los `futuros análisis´ que se mencionan. Al respecto, se estima que todas esas expresiones resultan suficientemente claras para entender su significado literal, excediendo el objeto de la ley 104 expedirse acerca de otras interpretaciones que puedan darse a las mismas. Apartados J/K/L/M/N: Conforme surge del propio texto del pliego técnico, la lista negra es una denominación de la base de datos de personas prófugas de la justicia. Por lo cual, las preguntas enunciadas ya han sido contestadas con anterioridad. Para más información ver: https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83|5qmQHYdlWCoEzPIKU0JAvRZ7kltC74K|7Tw11ctBR9dfFZZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObRlXsdfYAs0SFw==*" (nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-).

La parte actora indicó que se refirió a esta pregunta de modo conjunto con la 77, afirmando que "*el GCBA se limitó a pegar un link al pliego de las bases y*

condiciones para la contratación del SRFP…" (fs. 7 y 98).

Ahora bien, la presente pregunta consta de catorce subpreguntas, identificadas con letras según el orden del abecedario.

Cabe observar que el GCBA respondió únicamente algunas de dichas preguntas -a), b), f), j), k), l), m) y n)-, agrupándolas en dos conjuntos de preguntas: el primero a), b) y f); y el segundo j), k), l), m) y n). Luego, copió un link de la web.

Es decir que quedaron varias preguntas sin responder de manera específica, esto es: c), d), e), g), h) e i).

En cuanto al primer conjunto de preguntas -*a) ¿Qué se quiso decir con `detección de diferentes patrones de comportamiento´?; b) ¿Qué se quiso decir con `cambios de condiciones ambientales´?;* y *f) ¿En qué consisten esos `futuros análisis´ que se mencionan?*- el GCBA contestó que "*todas esas expresiones resultan suficientemente claras para entender su significado literal, excediendo el objeto de la ley 104 expedirse acerca de otras interpretaciones que puedan darse a las mismas*". Sin embargo, a criterio de este Tribunal dichas expresiones no son autoexplicativas y merecen algunas precisiones adicionales. Ninguno de dichos conceptos tienen significados unívocos y, ante la duda exteriorizada por el peticionante, por imperio de los principios *in dubio pro petitor* y buena fe (conf. art. 2º, segundo párrafo, ley 104), ameritan algún grado de esfuerzo explicativo por parte de la autoridad requerida.

En cuanto al segundo conjunto de preguntas *–j) ¿Quién realiza esta llamada `lista negra´?; k) ¿Cómo y que procedimiento se 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?* y *n) ¿Quién tiene permiso para modificar esta lista? ¿Qué parámetros o requisitos pide el sistema a efectos de modificar la lista?*- el GCBA contestó "[c]*onforme surge del propio texto del pliego técnico, la lista negra es una denominación de la base de datos de personas prófugas de la justicia. Por lo cual, las preguntas enunciadas ya han sido contestadas con anterioridad*". A criterio de este Tribunal, la respuesta brindada por el GCBA resulta absolutamente insuficiente. Tampoco termina de completarse consultando el link transcripto, el que remite al buscador de compras del GCBA, ni consultando el pliego de bases y condiciones acompañado en el archivo denominado "*9.- PLIEG-2019-10400885-GCABA-SSGA*", inserto en el soporte digital reservado a fs. 93, donde

únicamente refiere al tema de la lista negra al decir que el servicio deberá "[c]*ontar con una base de datos fotográfica de hasta cien mil (100.000) rostros para su posterior identificación formando una lista negra de personas buscadas*".

Finalmente, respecto del conjunto de preguntas no contestadas específicamente -*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?; 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?;* y *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?*-, se observa que el GCBA no dio satisfacción a los interrogantes allí planteados. Tampoco surge su respuesta del pliego de bases y condiciones acompañado en el archivo denominado "*9.- PLIEG-2019-10400885-GCABA-SSGA*", inserto en el soporte digital reservado a fs. 93.

En consecuencia, corresponde condenar al GCBA a brindar la información requerida mediante la pregunta 76 efectuada en sede administrativa por la parte actora.

V.15. Pregunta 77: ***En el mismo pliego se ha hecho una serie de manifestaciones genéricas que, dado el efecto que la interpretación que las mismas tendrían en los derechos fundamentales de las personas, hacen de suma importancia que se aclare. Así, se ha establecido los siguientes requisitos: `[…] Ante eventos repetitivos, el sistema deberá enmascarar automáticamente dichos eventos a modo de optimizar la visualización de 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 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 dalos de video, registrando la información de todas las personas que aparecen, permitiendo una búsqueda dinámica y veloz de las personas de interés. […]´…

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 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"?"

Al respecto, el GCBA contestó: "[l]*o enunciado en los párrafos previos, no corresponden a características técnicas del Sistema de Reconocimiento Facial de Prófugos. Estos conceptos devienen de la adquisición de otros software (predictivo y forense). Ver: https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83|5qmQHYdlWCoEzPIKU0JAvRZ7kltC74K|7Tw11ctBR9dfFZZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObRlXsdfYAs0SFw==*" (nota NO-2019-33745359-GCABA-DGEYTI de la DIRECCIÓN GENERAL DE ESTUDIOS Y TECNOLOGÍAS DE LA INFORMACIÓN del MINISTERIO DE JUSTICIA Y SEGURIDAD del GCBA -acompañada en soporte digital reservado por Secretaría a fs. 93-).

De la respuesta brindada, se extraen con toda claridad las falencias en que incurre del GCBA a la hora de brindar la información solicitada de manera pormenorizada, ya que la mera consulta del pliego de bases y condiciones particulares de la contratación del SRFP no basta para satisfacer las inquietudes, que son múltiples y variadas (dieciocho subpreguntas). En efecto, dicho pliego, acompañado por la demandada, no responde directamente las preguntas planteadas y, en consecuencia, resulta necesario un esfuerzo explicativo mayor por parte de la requerida.

Por lo tanto, corresponde condenar al GCBA a brindar la información solicitada mediante la pregunta 77 por la parte actora en sede administrativa.

VI. En consecuencia, corresponde intimar a la demandada GCBA a que brinde, en el plazo de diez (10) días, la información oportunamente requerida por la parte actora en sede administrativa de acuerdo con el análisis pormenorizado efectuado en el considerando precedente.

VII. Respecto a las costas, cabe imponerlas al GCBA por cuanto con su conducta obligó a la actora a iniciar este proceso y fue sustancialmente vencido (conf. art. 62 del CCAyT).

Por lo tanto, **RESUELVO**:

1º) Declarar abstracta el objeto de la demanda en relación con las preguntas 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 46, 48, 50, 51, 54, 57, 59, 60, 63, 64, 65, 68, 69, 70, 71, 72, 73, 74 y 75, de conformidad con lo explicado en el considerando **III**.

2º) Hacer parcialmente lugar a la demanda incoada por el OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO con relación a las preguntas 10, 13, 20, 26, 44 (segunda, tercera y cuarta parte), 45, 47, 52, 53, 58, 61, 62 (primera parte), 67, 76 y 77 de su pedido de acceso a la información al GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES, de conformidad con el desarrollo elaborado en el considerando **V**.

3º) Rechazar parcialmente la demanda en lo referido a las preguntas 44 (primera parte), y 62 (segunda parte) del pedido de acceso a la información, de conformidad con el desarrollo elaborado en el considerando **V.5** y **V.12**.

4º) Imponer las costas a la vencida (art. 62, CCAyT).

5º) Intimar a la demandada a brindar a la actora, en el plazo de diez (10) días, la información identificada en el punto2°.

6º) Regístrese y notifíquese a la parte actora por Secretaría a los correos electrónicos que surgen de autos (tanto al de la actora como al de su letrado apoderado) y al GCBA por Secretaría al correo electrónico notificacionesjudicialespg@buenosaires.gob.ar.

Francisco J. Ferrer

Juez

REGISTRADA AL TOMO_____FOLIO_____DEL LIBRO DE REGISTRO DE SENTENCIAS DEFINITVAS DE AMPARO DEL JUZGADO Nº 23 SECRETARÍA Nº 45. AÑO 2020. CONSTE.

Poder Judicial
Ciudad de Buenos Aires

JUZGADO N°23 - Expediente:9480/2019-0 CUIJ J-01-00050809-4/2019-0 - Actuacion: 14667141/2020

FIRMADO DIGITALMENTE 20/05/2020 14:16

Francisco Javier Ferrer
JUEZ/A
JUZGADO DE 1RA
INSTANCIA EN LO
CONTENCIOSO
ADMINISTRATIVO Y
TRIBUTARIO Nº 23