



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

Número:

Buenos Aires,

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

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

A: Fabiana Costanza (DGALSE),

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

De mi mayor consideración:

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

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

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

El Centro de Monitoreo Urbano (CMU) cuenta con un Protocolo de actuación sobre el Procedimiento en caso de alerta arrojada por el "Sistema de Reconocimiento Facial de 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° 5.688/16.

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

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

La auditoria del funcionamiento del Sistema de Reconocimiento Facial de 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 deviene en una alerta positiva son automáticamente descartadas del proceso de almacenamiento del sistema.

15) Una vez que las imágenes llegan al CMU, ¿cómo se cifra dicha información en el disco y en la memoria RAM? De no ser realizado este cifrado, ¿Qué medidas de seguridad, privacidad y confidencialidad son utilizadas para asegurar su control e integridad?

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

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

21) Informe si el software reconoce a menores de edad

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

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

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

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

No existe información que se comparta.

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

En total existen 114 usuarios.

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

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

15 usuarios con el perfil PFA Retiro.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Inmediatamente.

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

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

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

Los teléfonos institucionales no almacenan eventos.

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

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

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

46) ¿Qué policías reciben esta información?

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

47) ¿cuántos agentes reciben esta información?

El personal abocado por turno al servicio específico.

48) ¿En qué consisten estas alertas?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

La Secretaria de Administración de Seguridad y Emergencias.

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

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

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

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

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

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

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

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

Con respecto al Punto 1. (Objeto):

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

a. ¿Qué se quiso decir con “detección de diferentes patrones de comportamiento”?

b. ¿Qué se quiso decir con “cambios de condiciones ambientales”?

c. ¿Cuál es la cantidad de cámaras instaladas en la vía pública pertenecientes al gobierno de la Ciudad Autónoma de Buenos Aires y de la Policía de la Ciudad?

d. ¿Qué cantidad de esas cámaras permiten utilizar el software de reconocimiento facial?

e. ¿Qué tipo de encriptación se utiliza para el almacenamiento de esas imágenes que generen alertas?

f. ¿En qué consisten esos “futuros análisis” que se mencionan?

g. ¿Durante cuánto tiempo se guardarán dichas imágenes?

h. ¿Dónde se encuentran físicamente los servidores donde se almacena la información del registro resultante entre la inclusión de la base de datos de la CONARC con la del RENAPER, y la información de la estructura facial del rostro capturado por las cámaras instaladas en la vía pública de la Ciudad?

i. ¿Qué protocolos de seguridad son utilizados para el almacenamiento de la información del registro resultante entre la base de datos de la CONARC y el RENAPER, y lo grabado por las cámaras instaladas en la vía pública de la Ciudad?

j. ¿Quién realiza esta llamada “lista negra”?

k. ¿Como y que procedimiento se utiliza para la confección de la llamada “lista negra”?

l. ¿Cuántas personas hay en esta lista?

m. ¿Cuál es el criterio que se sigue para ingresar y/o egresar de esta lista?

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

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

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

Para más información ver:

<https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83l5qmQHYdlWCoEzPIKU0JAvRZ7klC74Kl7Tw1lctBR9dfFZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObRlXsdfYAs0SFw==>

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

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

- a. ¿Qué se considera como un "evento repetitivo" y qué criterios se utilizan para definirlo?
- b. ¿En qué consiste un "Área de Enmascaramiento" y como puede su consideración evitar "falsos positivos"?
- c. ¿A qué se refiere con "zonas de detección"? ¿Cuáles son estas zonas?
- d. ¿A qué se refiere con historia de los eventos? ¿Qué información se almacena? ¿Dónde es almacenada esta información? ¿Quién tiene acceso a esa información y por cuánto tiempo?
- e. ¿Qué información se considera como "purgable"? ¿Dónde se almacena esa información? ¿Cuáles son los plazos máximos y mínimos que se consideran a efectos de realizar esa purga?
- f. ¿Cuántos usuarios con los dos distintos permisos existen? ¿Qué cantidad de usuarios están limitados a la visualización de los datos? ¿Cuántos usuarios existen con total disponibilidad para todas las operaciones? ¿Quién otorga estos permisos? ¿De qué manera y con qué criterio se otorgan esos permisos?
- g. ¿Cuáles son la totalidad de las operaciones?
- h. ¿Qué criterio se utilizó a efectos de considerar que un 15% de falsos positivos era un porcentaje aceptable?
- i. ¿Quién determina las líneas virtuales mencionadas, y dónde se encuentran dichas líneas?
- j. ¿A qué se refiere con "zona estéril"?

- k. ¿Cuál es la cantidad (mínima) de personas y durante cuánto tiempo (mínimo) es necesario para que este se considere como hacinamiento?
- l. ¿En qué condiciones puede suceder un cruce de línea que implique un “acercamiento entre personas”? ¿Cuál es la utilidad práctica de esta categoría?
- m. ¿Cuánta es la cantidad mínima de personas necesarias para que se dé un caso de “merodeo”?
- n. ¿Qué se considera como “comportándose de una manera sospechosa”? ¿Cuáles son las actividades puntuales que el sistema está entrenado para reconocer? ¿Cómo se puede prever una actividad delictiva cuando se da este supuesto?
- o. ¿En qué consiste el presupuesto de “ocupación”? ¿Cuántas personas se necesitan como mínimo en un área para que se configure la ocupación? ¿Cuáles son los presupuestos fácticos de forma detallada para que se configure la ocupación? ¿Cuáles son aquellas áreas pasibles de ocupación?
- p. ¿En qué consiste la “tolerancia a los falsos positivos” mencionada?
- q. ¿Con que sin se recolecta la información acerca de la detección de emoción en el rostro de las personas? ¿Por qué se necesita detectar la emoción del rostro de las personas cuando el sistema sería utilizado exclusivamente para la detección de prófugos?
- r. ¿En qué consiste la indexación mencionada? ¿Qué se considera como “persona de interés? ¿Por qué razón se necesitaría registrar aquella información de estas “personas de interés”?

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

Ver:

[https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?
qs=BQoBkoMoEhyvzUss83|5qmQHYdlWCoEzPIKU0JAvRZ7kltC74K|7Tw11ctBR9dfFZZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObrIXsdfYAs0SFw==](https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83|5qmQHYdlWCoEzPIKU0JAvRZ7kltC74K|7Tw11ctBR9dfFZZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObrIXsdfYAs0SFw==)

Sin otro particular saluda atte.