G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
"2019 -Año del 25° Aniversario del reconocimiento de la autonomía de la Ciudad de Buenos Aires"

Número: NO-2019-25581723-GCABA-DGEYTI

Buenos Aires, Jueves 15 de Agosto de 2019

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

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

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

Con Copia A:

De mi mayor consideración:

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

1) ¿Cuántas cámaras de monitoreo posee la CABA?

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

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

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

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

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

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

Resolución 4k

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

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

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

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

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

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

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

El cifrado es Ipsec.

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

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

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

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

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

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

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

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

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

En DataCenter del MJyS.

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

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

21) Informe si el software reconoce a menores de edad

NO.

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

N/A

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

N/A

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

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

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

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

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

Teléfono institucional (POC) –

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

Los POC no almacenan eventos

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

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

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

Alertas arrojadas 3059.

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

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

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

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

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

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

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

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

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

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

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

Ver respuesta 61.

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

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

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

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

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

No.

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

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

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

Ver respuesta 61.

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

Ver pregunta 24

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

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

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

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

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

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

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

g. ¿Durante cuánto tiempo se guardarán dichas imágenes?

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

i. ¿Qué protocolos de seguridad son utilizados para el almacenamiento de la información del registro resultante entre la base de datos de la CONARC y el RENAPER, y

lo grabado por las cámaras instaladas en la vía pública de la Ciudad?

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

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

l. ¿Cuántas personas hay en esta lista?

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

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

https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83|5qmQHYdlWCoEzPIKU0JAvRZ7kltC74K|7Tw11ctBR9dfFZZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObRlXsdfYAs0SFw==

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

a. ¿Qué se considera como un “evento repetitivo” y qué criterios se utilizan para definirlo?

b. ¿En qué consiste un “Área de Enmascaramiento” y como puede su consideración evitar “falsos positivos”?

c. ¿A qué se refiere con “zonas de detección”? ¿Cuáles son estas zonas?

d. ¿A qué se refiere con historia de los eventos? ¿Qué información se almacena? ¿Dónde es almacenada esta información? ¿Quién tiene acceso a esa información y por cuánto tiempo?.

e. ¿Qué información se considera como “purgable”? ¿Dónde se almacena esa información? ¿Cuáles son los plazos máximos y mínimos que se consideran a efectos de realizar esa purga?

f. ¿Cuántos usuarios con los dos distintos permisos existen? ¿Qué cantidad de usuarios están limitados a la visualización de los datos? ¿Cuántos usuarios existen con total disponibilidad para todas las operaciones? ¿Quién otorga estos permisos? ¿De qué manera y con qué criterio se otorgan esos permisos?

g. ¿Cuáles son la totalidad de las operaciones?

h. ¿Qué criterio se utilizó a efectos de considerar que un 15% de falsos positivos era un porcentaje aceptable?

i. ¿Quién determina las líneas virtuales mencionadas, y dónde se encuentran dichas líneas?

j. ¿A qué se refiere con “zona estéril”?

k. ¿Cuál es la cantidad (mínima) de personas y durante cuánto tiempo (mínimo) es necesario para que este se considere como hacinamiento?

l. ¿En qué condiciones puede suceder un cruce de línea que implique un “acercamiento entre personas”? ¿Cuál es la utilidad práctica de esta categoría?

m. ¿Cuánta es la cantidad mínima de personas necesarias para que se dé un caso de “merodeo”?

n. ¿Qué se considera como “comportándose de una manera sospechosa”? ¿Cuáles son las actividades puntuales que el sistema está entrenado para reconocer? ¿Cómo se puede prever una actividad delictiva cuando se da este supuesto?

o. ¿En qué consiste el presupuesto de “ocupación”? ¿Cuántas personas se necesitan como mínimo en un área para que se configure la ocupación? ¿Cuáles son los presupuestos fácticos de forma detallada para que se configure la ocupación? ¿Cuáles son aquellas áreas pasibles de ocupación?

p. ¿En qué consiste la “tolerancia a los falsos positivos” mencionada?

q. ¿Con que sin se recolecta la información acerca de la detección de emoción en el rostro de las personas? ¿Por qué se necesita detectar la emoción del rostro de las personas cuando el sistema sería utilizado exclusivamente para la detección de prófugos?

r. ¿En qué consiste la indexación mencionada? ¿Qué se considera como “persona de interés? ¿Por qué razón se necesitaría registrar aquella información de estas “personas de interés”?

https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83|5qmQHYdlWCoEzPIKU0JAvRZ7kltC74K|7Tw11ctBR9dfFZZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObRlXsdfYAs0SFw==

Sin otro particular saluda atte.

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

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

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