SOLICITUD DE ACCESO A INFORMACIÓN PÚBLICA

Ministerio de Seguridad y Justicia
De la Ciudad Autónoma de Buenos Aires
At. Ministro de Seguridad y Justicia
Sr. Diego Santilli
S_____/_____D

El **OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO**, con domicilio en (eliminado por cuestiones de privacidad) y constituyendo domicilio electrónico en odiaasoc@gmail.com, se presenta ante Vd. y dice:

1. PERSONERÍA

Conforme surge de la copia del estatuto del OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO, que se adjunta al presente como Anexo I, de ahora en más "O.D.I.A.", somos una Asociación Civil debidamente inscripta en el Registro de la Inspección General de Justicia bajo el número 213, del libro "2 AC", de Asociaciones Civiles.

2. OBJETO

En virtud de ello, venimos a promover una formal petición de acceso a la información pública en los términos de lo dispuesto por la Ley N° 104 de Acceso a la Información Pública.

Lo que pretendemos a través de esta petición es conocer determinada información acerca del llamado "Sistema de Reconocimiento Facial de Prófugos" que, según se ha hecho saber a la ciudadanía en diversas publicaciones en la prensa, estaría funcionando en 300 cámaras de la Ciudad Autónoma de Buenos Aires.

3. PETICIONES

El 3 de abril de 2019 se llevó a cabo el 1er Congreso Internacional sobre "Combate del Delito Transnacional y los Procesos de Integración". En dicho Congreso, el vicejefe de gobierno de la Ciudad Autónoma de Buenos Aires adelantó que ese mismo mes iba a empezar a funcionar en el territorio de la ciudad un sistema de reconocimiento facial que sería utilizado solamente para identificar supuestos prófugos de la justicia.

Sin demasiadas explicaciones, además de aquellas manifestaciones genéricas, en fecha 24 de abril de 2019 se publicó la Resolución N° 398/MJYSGC/19 (de ahora en más "Resolución 398/19") mediante la cual se habría aprobado la implementación de un "Sistema de Reconocimiento Facial de Prófugos". De la lectura de aquella normativa, nos surgen las siguientes incógnitas:

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 las 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 son 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 borra?

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 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?

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 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 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 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 correo señalado en el encabezado) del convenio de confidencialidad que sería firmado por el personal que operaría el sistema.

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

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

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

En el último párrafo del art. 5 del Anexo se establece lo siguiente: "*[...] La Policía de la Ciudad no está autorizada a ceder tales archivos a ninguna otra autoridad administrativa de la Ciudad, con excepción del Ministerio de Justicia y Seguridad el que tampoco podrá utilizarlos para finalidades distintas a aquéllas que motivaron su obtención.*"

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

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

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

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

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

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

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

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

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

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

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

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

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 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?

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

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

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 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?

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

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

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

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

74) Copia del convenio realizado entre el Gobierno de la Ciudad de Buenos Aires y el CONARC para el envío de las imágenes, archivos, e

informaciones correspondientes y relacionadas a este Sistema de Reconocimiento Facial.

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

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?

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 áre****a. […]*" "*[…] 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"?

4. PETITORIO

En virtud de lo expuesto a lo largo de este Pedido de Información, le solicitamos cordialmente tenga a bien proveernos de la información solicitada.

Sin otro particular, lo saludamos atentamente.

Observatorio de Derecho Informático Argentino.