Auditoría al Sistema de Reconocimiento Facial de Prófugos (SRFP)

Plan de Trabajo – Defensoría del Pueblo de CABA

Estado actual. Mandato judicial

El fallo judicial de *primera instancia* indicó que resulta necesario que al momento de ser implementado el Sistema de Reconocimiento Facial de Prófugos (SRFP): a) se cuente con los mecanismos de control de este sistema, es decir se constituya la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia y que la Defensoría del Pueblo como órgano de control pueda ejercer eficazmente sus funciones; b) se constituya el registro de datos relativo al sistema de videovigilancia; c) se realice un estudio previo relativo al impacto sobre los datos personales y d) se convoque a la ciudadanía a debatir las cuestiones relativas al Sistema de Reconocimiento Facial de Prófugos. Pues, lo contrario se traduce en graves consecuencias sobre los derechos de las personas que transitan la Ciudad.

Además, según la sentencia dictada por la Sala I de la Cámara de Apelaciones en lo CATyRC, en autos "Observatorio de Derecho Informático Argentino O.D.I.A. y otro c/GCBA s/amparo", la rehabilitación del funcionamiento del SRFP quedó supeditada a la realización de las investigaciones y pruebas necesarias sobre el software que utiliza el SRFP (por parte de los organismos de control con asistencia del accionado o de quien éste considere adecuado), para determinar si su empleo tiene un impacto diferenciado según las características personales de los individuos afectados.

Requerimientos y plan de trabajo por etapas

En el marco de las sentencias citadas, a continuación se presentan algunos lineamientos breves, que tienen como objetivo establecer las bases para cumplir con el mandato judicial. Cabe aclarar que en esta propuesta no se incluye el proceso de apertura a la ciudadanía, indispensable para la posible

puesta en funcionamiento del sistema, sin perjuicio de lo cual la Defensoría podría participar en la medida de sus competencias.

El siguiente plan de trabajo se concibe como un conjunto, que se distingue en tres etapas interrelacionadas: la primera, responde a la necesidad de que el Gobierno de la Ciudad de Buenos Aires brinde información específica que permita a la Defensoría caracterizar ciertos aspectos centrales del funcionamiento integral del sistema y su situación actual; la segunda, incumbe a la auditoría sobre el software y sus especificidades técnicas, para lo cual se requerirá la asistencia de la Facultad de Ciencias Exactas de la Universidad de Buenos Aires y la apertura y colaboración de las autoridades y responsables directos del sistema del GCBA; por último, se llevará a cabo una evaluación de la información recopilada con el objetivo de elaborar un informe general de evaluación y recomendaciones de política pública.

Etapas de trabajo (especificaciones)

1era Etapa – Acceso a la información

Se enviarán oficios solicitando información al Ministerio de Seguridad del GCBA y/u otras áreas que correspondieran.

En el **Anexo I** se muestra una primera lista de preguntas sobre el funcionamiento, estadísticas, informes y protocolos existentes sobre el SRFP.

2da Etapa – Pericial

A partir de un convenio específico entre la Defensoría del Pueblo de la Ciudad de Buenos Aires y la Facultad de Ciencias Exactas de la Universidad de Buenos Aires, se constituirá un equipo de especialistas para llevar a cabo una auditoría sobre el software del SRFP.

Las pericias se enfocarán en el análisis sobre los posibles sesgos que pueda contener el diseño del sistema. En este punto, se recoge el mandato de la Cámara de Apelaciones, que ordena determinar si el empleo de esta herramienta tiene un impacto diferenciado según las características personales de los individuos afectados. No obstante, se podrán indagar otros aspectos

relacionados a fin de comprender el funcionamiento global del SRFP y sus posibles impactos en la privacidad de las personas.

A tal fin, es condición necesaria que el Gobierno de la Ciudad acepte prestar colaboración atendiendo a los requisitos técnicos elaborados por el equipo de especialistas de la facultad de Ciencias Exactas de la UBA, consultado por este organismo (se detallan en el Anexo 2).

3era Etapa – Informes

Se elaborará un informe de evaluación final, a partir de los datos recabados y los resultados periciales. Asimismo, se contemplarán posibles recomendaciones respecto a los usos del SRFP, riesgos, potencialidades, resguardos necesarios y cualquier otro aspecto que surja del análisis, con la mira puesta en el respeto de los Derechos Humanos y la privacidad de la ciudadanía.

ANEXO I

Tengo el agrado de dirigirme a usted en mi carácter de Defensora del Pueblo de la Ciudad Autónoma de Buenos Aires, en el trámite nro. 2068/19 iniciado de oficio con el fin de analizar la implementación del Sistema de Reconocimiento Facial de Prófugos (en adelante SRFP) y en el marco de lo ordenado a través de la sentencia dictada por la Sala I de la Cámara de Apelaciones en lo CATyRC, en autos “Observatorio de Derecho Informático Argentino O.D.I.A. y otro c/GCBA s/amparo”, solicito a usted se expida sobre los siguientes tópicos:

1-Informe el estado actual de la contratación realizada en el año 2019 mediante pliego N° 2019-10400885-GCABA-SSGA y Resolución 59/SSGA/19 por medio de la cual se habilito la adquisición del software de SRFP.

2-Realice una descripción general del funcionamiento del software únicamente con relación al SRFP.

3- Informe cantidad de licencias que serán utilizadas y ubicación de todo tipo de dispositivos sobre los cuáles se montarán.

4.-Atento las previsiones de los principios del Libro VII Título I de la Ley 5688, adjunte evidencia, estudios e informes que justifiquen la decisión de implementar el SRFP en los lugares en los se prevé su funcionamiento (subterráneos, eventos deportivos, etc);

5.-Toda vez que en la causa judicial se adjuntó un “Convenio Específico de Colaboración sobre Relevamiento y Auditoria de Seguridad entre el Ministerio de Justicia y Seguridad del Gobierno de la Ciudad Autónoma de Buenos Aires y la Universidad de la Plata” informe el estado actual del mismo y en tal caso adjunte el informe resultado de la auditoría encargada a dicha Universidad.

6.-En relación al desempeño del SRFP, atendiendo a que su objetivo es el de la identificación y reconocimiento de personas buscadas por orden judicial, indique cual será el índice de semejanza (en porcentaje) ante la identificación de un rostro.

7.-Oportunamente este Órgano puso de relieve las serias falencias en la base de datos de CONAaRC y las afectaciones que estas ocasionaban a derechos de los ciudadanos, toda vez que se detectó la detención de personas que finalmente no resultaron ser las requeridas judicialmente informe qué medidas correctivas se adoptaron o se adoptaran en el futuro.

8.-Teniendo en cuenta la experiencia recogida durante el tiempo en el cual se implementó el SRFP, informe si se prevé realizar o si se ha realizado un estudio de impacto a la privacidad y en su caso remita copia certificada de los resultados.

9.-Remita un informe estadístico del periodo de funcionamiento del SRFP, detallado: a) cantidad de alertas generadas; b) cantidad de personas notificadas (en los que existía orden judicial vigente de notificar de alguna medida como comparendo, citación, audiencia, etc sin que el juzgado dispusiera su detención); c) personas identificadas respecto de las cuales la medida se encontraba sin efecto; d) personas que fueron detenidas por estar la medida restrictiva vigente; e) personas que fueron interceptadas sin coincidencia de datos (falsos positivos) y f) personas que fueron interceptadas pero no era la persona requerida judicialmente (DNI erróneo, etc)

10.-Con relación al funcionamiento del CMU informe cantidad de operadores del SRFP, indicando nombre, apellido, DNI y funciones específicas que cumplen, horarios y toda otra medida de interés. Remita convenios de confidencialidad suscriptos en relación al tratamiento de dato sensible.

11.-Informe si se han elaborado manuales o protocolos para determinar funciones y responsabilidades dentro del Centro de Monitoreo Urbano con relación al SRFP. En su caso, remita copia certificadas de los mismos.

12.-Informe si se han elaborado protocolos de actuación con relación al procedimiento que debe realizar el personal policial que procederá a interceptar a una persona respecto de la cual el SRFP hubiera emitido una alerta. En su caso, remita copia certificada de aquellos.

13.-Con el fin de garantizar los derechos de la ciudadanía, informe si se han adoptado o adoptaran medidas de transparencia tales como la instalación de cartelería que informe sobre la utilización del SRFP.

14.- Con respecto al funcionamiento del sistema, especifique cuál es la arquitectura de la solución tecnológica utilizada, detallando los servidores empleados, las aplicaciones, etc.

15.- Indique de qué manera son tratados los datos dentro del SRFP, qué tipo de datos son almacenados y por cuánto tiempo, cómo se protege su seguridad, si los datos sensibles cuentan con una protección especial y cómo es la dinámica del flujo de los mismos.

16.- Realice una descripción pormenorizada del procedimiento y tratamiento de los datos en los casos de ausencia de match en el sistema de reconocimiento facial. Especialmente si los mismos son almacenados, por cuánto tiempo y con qué fines.

17.- Especifique si, en caso de ser solicitado por autoridad competente, el sistema actual es técnicamente capaz de realizar la búsqueda de una persona particular que no se encuentra dentro de la base de datos de CONAaRC. Detalle si hubo casos en este sentido.

ANEXO 2

Requerimientos básicos para poder realizar una auditoría del software de reconocimiento facial de profugos del Gobierno de la Ciudad de Buenos Aires.

El requerimiento principal para poder evaluar el sistema de manera correcta y exhaustiva es que los datos sean representativos, en todo aspecto, de los datos en los que sería usado el sistema en la práctica. En esta tarea los datos están compuestos por: a) imágenes tomadas con cámaras en la calle, b) fotos de personas de interés. Los requerimientos para estos dos sets de datos son:

1. Los datos de las cámaras deben ser tomados con las mismas cámaras en los mismos lugares en que estarían si el sistema fuera puesto en uso. No es necesario tener datos de cada posible cámara pero sí que sea una muestra representativa. Por ejemplo, que no sean todas las cámaras de un mismo barrio sino que estén distribuidas de manera uniforme en toda la región de interés.

2. Las fotos de las personas de interés también deben ser representativas de la población de Argentina y tomadas con la misma perspectiva, resolución e iluminación que las que serían usadas eventualmente. Es necesaria una muestra que incluya rostros con distintas combinaciones de género, rango etario y etnia para la cual puede ser usado el sistema. Estimamos que sería necesario tener al menos 100 fotos de cada combinación de esas tres características.

3. Para cada combinación de esas tres características es necesario que haya suficientes coincidencias (al menos 50, idealmente más) con una o más imágenes de las cámaras para tener casos positivos en los que evaluar.

Queremos enfatizar que es importante que las coincidencias entre las imágenes de las cámaras y las fotos de las personas de interés sean anotadas con certeza. No deberían ser anotadas por un humano mirando esas mismas imágenes ya que es probable que el humano cometa los mismos errores que el sistema. Es necesario conocer la identidad real de las personas en las cámaras para asegurarse que efectivamente corresponden a una de las personas de interés.

Finalmente, necesitamos poder correr el sistema en los datos provistos o, en su defecto, que nos den las salidas. La primera opción es preferible para que podamos saber, por ejemplo, si el sistema genera siempre la misma salida ante las mismas entradas.

Más allá de esos datos necesarios para la evaluación del sistema, sería ideal contar con una descripción detallada de cómo fue entrenado y desarrollado el sistema, qué tipos de datos fueron usados para ambas cosas y qué proceso se usó en el desarrollo.