

MANIFIESTA.

PRESENTA OBSERVACIONES. PROPONE MEDIDAS.

Sra. Jueza,

La Fundación para la Difusión del Conocimiento y el Desarrollo Sustentable “Vía Libre” (en adelante “Fundación Vía Libre”), representada en este acto por María Beatriz Busaniche, en calidad de Presidenta de la mencionada institución, con el patrocinio letrado de Margarita Trovato (T° 133 F° 719 CPACF), manteniendo el domicilio legal constituido y domicilio electrónico en el usuario XXXXXXXX, en la causa caratulada “Observatorio de Derecho Informático Argentino O.D.I.A. y Otros c/ G.C.B.A. s/ amparo – Otros”, Expte. N° 182908/2020-0, a V.S. respetuosamente decimos:

I. Objeto

Venimos a acercar al Tribunal, en calidad de amicus curiae, nuestras observaciones a la Licitación Pública N° 3202-0750-LPU26, prevista para “la contratación del servicio de reconocimiento facial y gestión de alertas en imágenes de video, bajo la modalidad de Orden de Compra Abierta” por parte del GCBA, en función del expediente administrativo acompañado en autos (documento PDF anexo a la Actuación Nro. 2202645/2026), en continuidad de lo discutido en la audiencia del día 25/09/2026.

II. Sobre los Pliegos de Bases y Condiciones Particulares (PBCP) y de Especificaciones Técnicas (PET). Su adecuación a las sentencias de autos.

En el caso de autos, la Cámara de Apelaciones en lo CATyRC ordenó en su decisión del 28/04/2023 (Actuación nro. 1055665/2023), confirmatoria de la sentencia de este Juzgado del 07/09/2022 (Actuación nro. 2453371/2022), suspender el SRFP hasta que se verificara: 1) la constitución y debido funcionamiento de los órganos de control, 2) “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 este considere adecuado), para determinar si su empleo tiene un impacto diferenciado según las características personales de los individuos afectados”, y 3) la publicidad e información a los vecinos y organizaciones que así lo solicitaran sobre la existencia de la herramienta, su funcionamiento y las reglas jurídicas que en su totalidad lo rigen, a fin de que expongan las observaciones que consideren necesarias (Cfr. puntos resolutivos 3 y 4 de la mencionada sentencia). En lo que aquí nos interesa retomar, el punto 2 quedó frenado por la imposibilidad de avanzar en una auditoría sobre el funcionamiento del sistema, en tanto su código fuente y otra información técnica relevante no fueron aportados al expediente.

En paralelo, el GCBA informó en el expediente la voluntad de abrir una licitación pública para contratar un nuevo servicio de software que cumpla esta función, a cuyos efectos se celebró el 25 de septiembre del año en curso una audiencia judicial. Como manifestamos en esa oportunidad, valoramos positivamente la voluntad de intentar una nueva contratación bajo los lineamientos de aquella decisión judicial y que se hayan incorporado salvaguardas relevantes. Sin embargo, como también aclaramos, persisten deficiencias graves, que vuelven difícil

imaginar un sistema que, al desplegarse, sea efectivamente respetuoso de los lineamientos que sentaron las sentencias de Primera Instancia y de Cámara en el caso de autos.

No desconocemos la buena voluntad ni los avances incorporados sino que entendemos que, tal como están redactados los pliegos hoy, no los vuelve exigibles ni verificables. Siguiendo el compromiso asumido por Fundación Vía Libre en aquella oportunidad, presentamos a continuación una serie de observaciones y de recomendaciones de mejora al pliego en cuestión.

Para ordenar el desarrollo, las dividimos en problemas respecto de las especificaciones técnicas y los procesos de auditabilidad, y en los impactos en derechos, específicamente en protección de datos personales. Al final de cada punto ofrecemos una propuesta de mejora, sin perjuicio de que en el apartado III nos referiremos en particular a las condiciones que consideramos mínimas para una evaluación de impacto respetuosa de los estándares internacionales.

II.a. El PET contiene especificaciones imprecisas e incorrectas, y omisiones graves.

Incluso cuando el Pliego de Especificaciones Técnicas (PET) aborda cuestiones técnicas relevantes, lo cierto es que lo hace de forma vaga, imprecisa y, en algunos casos, incorrecta. Además, omite información sobre elementos esenciales del funcionamiento. En detalle:

II.a.1. El PET no prevé cómo evaluar ni mitigar sesgos.

Uno de los fundamentos centrales que justificó la suspensión del sistema contratado originalmente por el GCBA es la existencia de sesgos que podrían derivar en un impacto diferenciado en ciertos grupos de personas en función de su aspecto físico. Estos sesgos derivan de la propia tecnología, pero se agravan notablemente cuando los materiales con que fue entrenado el sistema no contienen la diversidad suficiente para mitigar el trato discriminatorio contra la diversidad de poblaciones residentes y que transitan en la Ciudad de Buenos Aires. El pliego actual no resuelve de manera suficiente esta preocupación.

En concreto, remite a los Lineamientos Operativos para la Gobernanza y Uso Responsable de Sistemas y Agentes de Inteligencia Artificial en el ámbito del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires (en adelante “Lineamientos Operativos”), aprobados por Resolución N° 98/SECITD/26 del GCBA, pero muchas de sus enumeraciones son retóricas y no se traducen en exigencias concretas. A esta altura del proceso, todo aquello que no suponga una obligación contractual para la firma proveedora del sistema podría ser eludido con justificaciones típicas como la opacidad de los sistemas algorítmicos, la propiedad intelectual o la imposibilidad de aportar información técnica por secretos industriales o por la subcontratación de proveedores externos. En este sentido, es imprescindible que las obligaciones que este tribunal ha fijado como parte indispensable de la potencial implementación no se vuelvan opcionales o meras declamaciones a la hora de efectivizar una contratación de sistemas informáticos.

En concreto, los “Lineamientos Operativos” requieren, por un lado, documentar el “origen, calidad, limitaciones, transformaciones relevantes y eventuales riesgos de sesgo” de los datos de entrenamiento de los sistemas y las medidas para mitigarlos (art. 5). También prevén “la evaluación y mitigación de sesgos en datos de entrenamiento, ajuste y operación” (art. 4, principio i.) y la “revisión de sesgos” entre los mecanismos de monitoreo (art. 13). Sin embargo, estas cuestiones no están incorporadas de manera concreta al PET, cuyo único

requisito en este sentido es la exigencia genérica de una tasa de falsos positivos “no mayor al cinco por ciento (5%)” que, como veremos a continuación, es problemática en sí misma.

A su vez, exigen una evaluación documentada (art. 11), que el Pliego de Bases y Condiciones Particulares (PBCP) dice que se cumplirá a través de una prueba funcional y su informe técnico. Pero lo cierto es que esa prueba no mide sesgos ni impacto diferencial, sino que se basa en “las métricas de desempeño informadas por los oferentes” (art. 24.3.4 de la última versión del PBCP, p. 580 en adelante). Además, aclara que no sustituye “las evaluaciones y controles que correspondan con carácter previo a la puesta en funcionamiento operativo” (art. 25), pero no dice cuáles serán estos.

II.a.2. El límite de falsos positivos

Si bien el PET **establece un límite del 5% de falsos positivos**, que discursivamente podría parecer un buen criterio, tiene en realidad una serie de problemas importantes.

En primer lugar, la elección del “5%” es arbitraria (o al menos no se explicó lo contrario): ¿por qué 5% está bien y no 2%, o 0.1%, o 20%? Si bien la justificación no debe estar necesariamente contenida en el pliego (la motivación no incumbe al oferente), sí es una laguna para el control ciudadano. ¿Qué estándar o experiencia comparada se está mirando para fijar este número?

Por otro lado, no se explicita en el PET si se refiere al 5% de falsos positivos sobre el total de inferencias que hace el sistema (es decir, cada rostro que escanea cada cámara) o 5% de las alertas emitidas. Técnicamente, la forma estándar suele ser medir sobre el total de inferencias, pero en la audiencia de referencia el GCBA expresó que el 5% sería medido únicamente sobre las alertas emitidas¹. Esto implica una forma de medir “no estándar”, y que arroja un número muy distinto. Esto sí debería ser precisado en el pliego y no quedar únicamente sujeto a lo que se dijo oralmente en aquella oportunidad.

En tercer lugar, en ningún momento se fija el nivel de ajuste de falsos negativos con el que se mide: esto implica que los falsos positivos podrían bajarse a costa de aumentar los falsos negativos, por lo que la tasa de falsos positivos podría ser “correcta” pero sin que conozcamos a qué costo se llegó a ese resultado. Por ejemplo, se podría ofertar un sistema que nunca levante alertas y cumplir perfectamente con el pliego: 100% de falsos negativos.

Por último, tampoco se desagrega por grupo demográfico, ni se prevé la metodología de medición o una instancia de validación independiente. Esto implica en los hechos que la cifra dependerá de cómo se configure el sistema. Además, una tasa agregada del 5% puede ocultar tasas mucho más altas para poblaciones específicas: sabemos que la tecnología de reconocimiento facial tiene tasas de error documentadas más altas para mujeres, personas racializadas y personas trans, por ejemplo. Al exigir en abstracto un porcentaje máximo de falsos positivos, no se contemplan estas variables.

¹ La manera estándar de calcular el ratio de falsos positivos es la siguiente: $RFP = \frac{FP}{FP + Verdaderos\ Positivos}$ (ratio de falsos positivos) = FP (falso positivo) / (FP + Verdaderos Negativos). En cambio, lo que se desprende de la audiencia es que en este caso se mediría $RFP = FP/FP + Verdaderos\ Positivos$. El resultado es muy distinto.

En el mismo sentido, el PET tampoco aclara cómo se medirá el video: cuál será la posición de la cámara, cómo se contempla la falta de colaboración de la persona filmada (no es, por ejemplo, el caso voluntario de una persona que “mira a la cámara” al pasar migraciones en un aeropuerto) o el contexto en el que se despliega (persona aislada o multitud). Tampoco define el criterio de comparación, es decir, entre qué resultados se toma el mejor.

En este escenario, no se prevé un mecanismo para corregir los falsos positivos, es decir, un circuito para que esa información sirva para corregir el sistema, por lo que podría seguir detectando mal a la misma persona. Esto se relaciona con el monitoreo y la revisión continuos que prevé el art. 13 de los “Lineamientos Operativos”, que fue destacado en la audiencia junto con su título IV, sobre implementación y mejora continua. Sin embargo, no se traduce en exigencias o mecanismos concretos exigibles en el Pliego.

En aquella oportunidad hicimos referencia a un modelo de evaluación que podía ser adoptado en este sentido: nos referimos a la suite de evaluación FIVE (Face in Video Evaluation), edición 2024, un programa oficial del Instituto Nacional de Estándares y Tecnología de Estados Unidos diseñado para medir la precisión y robustez de los algoritmos de reconocimiento facial en secuencias de video². Quedamos a disposición de V.S. para acompañar al Tribunal en el seguimiento de este proceso (u otro similar) si se decidiera adoptarlo.

II.a.3. Elementos esenciales del funcionamiento no están en el PET.

Por otro lado, hay características centrales que el Ministerio de Seguridad comentó en la audiencia pasada pero que el pliego no contempla formalmente.

Allí se conversó, por ejemplo, sobre cómo llegan las imágenes al sistema y cómo funciona el proceso de cotejo (cómo se convierte en un vector, qué es lo que se compara, qué se almacena y dónde). Se dijo, en este sentido, que las alertas pasan por una instancia de intervención humana del área de biometría de la Policía, que las coteja con sus propias imágenes antes de cualquier detención. Esto dependería directamente de regulaciones sobre la actuación policial que excederían el pliego en cuestión. Sin embargo, es central conocer en detalle tanto el proceso técnico como el procedimiento de “despliegue” de la tecnología, con la actividad humana que implica, que debe estar debidamente reglamentada y entendida como parte integrante del mismo proceso.

De hecho, a esto se refirió el perito experto Sebastián Uchitel al explicar que no se puede evaluar si el sistema es seguro sin información de contexto sobre cómo se implementa: un “*safety assurance case*” requiere un argumento sobre por qué no habrá resultados arbitrarios, y eso depende de toda la “capa de aplicación” y no solo del sistema técnico, que es de lo que habla el pliego. Sobre este punto en particular, el pliego debería pedir expresamente un “*safety assurance case*” como parte del entregable.

Consideramos indispensable que se refuercen los requerimientos técnicos en este sentido, que se describa de manera explícita todo el proceso de aplicación y funcionamiento de la comparación de imágenes. Al mismo tiempo, deben incluirse las regulaciones o resoluciones de actuación policial que el Ministerio mencionó, de modo tal que pueda evaluarse también el contexto en el que se encendería el sistema.

² Para información ver https://pages.nist.gov/frvt/html/frte_five.html

II.a.4. La auditoría prevista en el PET y en el PBCP no alcanza al motor algorítmico del sistema.

El PET exige una declaración jurada del adjudicatario que autorice el acceso al código fuente “de los procesos de integración de datos” y un registro permanente e inalterable de altas, bajas y modificaciones de los registros de prófugos (art. 6 de la última versión del PET, p. 628 en adelante). A esto, el Pliego de Bases y Condiciones Particulares (PBCP) agrega como requisito una carta compromiso, avalada por el fabricante, de dar acceso al código del “software de los procesos de integración de datos”, para “eventualidades de índole legal o requerimientos de seguridad informática” (PBCP, art. 24.3.7). De aquí se desprenden dos problemas: por un lado, que únicamente se acceda a este código para eventualidades legales o informáticas, es decir, en formato “excepción”, y no como una regla general que garantice la auditabilidad que exigen las sentencias de Primera Instancia y de Cámara de este proceso. Por otro lado, como se discutió en la audiencia de referencia, queda por fuera el código fuente del motor algorítmico del sistema de Inteligencia Artificial, y por lo tanto también el acceso a los datos con que fue entrenado y su desempeño por subgrupo poblacional.

Además, como también se abordó en aquella oportunidad, es muy preocupante que el pliego deje en cabeza de la empresa la auditoría, dándole el formato de “declaración jurada” sin mayores obligaciones. Cuando se trata de defender los derechos de la ciudadanía, el control no debe ser opcional o ficticio. El Pliego tampoco aclara quién será responsable de evaluar esa auditoría o la validez de la mencionada declaración jurada, con qué periodicidad se debe realizar ni si los resultados se harán públicos; únicamente se menciona el derecho del Ministerio de auditar el cumplimiento de las obligaciones contractuales y legales (PBCP, art. 65).

Entregar el código debería ser una obligación de la empresa, establecida como cláusula de la licitación, y debería referir al funcionamiento del motor algorítmico, incluyendo con qué datasets se entrenó el sistema y cómo está representada en ellos la demografía buscada, lo que tiene impacto directo en los sesgos inherentes a todo el sistema. Mientras no se establezcan condiciones claras, el sistema seguirá siendo inauditable en la práctica.

II.a.5. Falta información sobre las pruebas de funcionamiento

El Ministerio dijo en la audiencia que las pruebas se harán con todos los oferentes antes de avanzar en la contratación y que probar el sistema requeriría el permiso de la jueza. El art. 25 del PBCP prevé una maqueta entregada antes de la apertura de ofertas, con pruebas “a cargo de los oferentes”, cuyos resultados documenta la Dirección General Activos Digitales, Tecnología e Informática del Ministerio de Seguridad, para la Comisión de Evaluación de Ofertas, que tiene a cargo evaluar los resultados de la prueba funcional para decidir la adecuación técnica de cada oferta. Pero no regula quién más puede participar de la prueba, cómo se documenta más allá de ese informe ni con qué criterio se la considera “satisfactoria”, expresión que aparece en el PET como condición previa a la puesta en funcionamiento (art. 11.b.).

Sobre este punto, consideramos fundamental formalizar los criterios de evaluación y las instancias de participación ciudadana, no sólo en cumplimiento de los principios generales de transparencia y auditabilidad, sino de la propia sentencia del caso de autos.

Es indispensable que en esta instancia también estén conformados los órganos de contralor y que tengan plena participación en esta instancia del proceso.

II.a.6. Sobre la evaluación de impacto en privacidad

La evaluación de impacto -elemento central cuya ausencia justificó la suspensión del sistema actual- que se exige en el PET en cuestión es un formulario genérico, que está a cargo del adjudicatario, debe ser presentada de forma posterior a la adjudicación y a la marcha blanca, y no tiene previsto ningún mecanismo de evaluación o aprobación.

En concreto, el “Informe de Evaluación de Impacto en la Privacidad (PIA)” consta en el Anexo I del PET y está basado en normas ISO/IEC 29134 (última versión anexa en p. 641 y ss.). Se trata de un formulario con campos por completar (“Describir...”, “Indicar...”) y seis riesgos genéricos preimpresos, sin contemplar ningún contenido específico de un sistema de reconocimiento facial. Además, su lista de anexos menciona una serie de normas aplicables, como ISO/IEC 29100 y el Reglamento General de Protección de Datos de la Unión Europea, pero no incluye la Ley Nacional de Protección de Datos Personales 25.326 ni la Ley 1.845 de la Ciudad.

Luego, el PET dispone que sea la empresa adjudicataria la que elabore y presente la EIPD, y lo haga una vez “concluida la etapa de marcha blanca (período de prueba final)” (PET, art. 5). Esto invierte la lógica de una evaluación de impacto, que debe ser previa a la decisión de implementar: los propios “Lineamientos Operativos” exigen la evaluación documentada “antes de la adquisición, desarrollo, prueba piloto o implementación” (art. 11). Resulta especialmente grave porque el propio Anexo I identifica como algunos de los motivos que justifican realizar una evaluación de impacto al tratamiento de categorías especiales de datos (que incluye biometría), al “uso de nuevas tecnologías” y a la “monitorización sistemática de espacios de acceso público” (punto 3 de la planilla modelo para la evaluación, Anexo I), todas características que este sistema reúne, y sin embargo no se requiere la evaluación antes de su despliegue. Peor aún, si bien se establece que se presente una vez “concluida la etapa de marcha blanca”, el pliego no fija un plazo máximo para presentarla ni define qué es concretamente la marcha blanca.

Entre las condiciones previas a la puesta en funcionamiento (que será con autorización expresa del Ministerio de Seguridad, hasta 90 días después de la aprobación de la prueba funcional), el PET solo exige “la presentación de la EIPD conforme Anexo I”, sin requerir que esa evaluación sea auditada, revisada o aprobada por ninguna autoridad u organismo. En este sentido, el Anexo I tiene campos para el responsable de protección de datos, para quien “revisó” el informe y para una recomendación final sobre la procedencia, pero no dice quién la revisa ni qué efecto tendría un resultado negativo.

Lo cierto es que la evaluación no puede quedar únicamente a cargo del adjudicatario (p. 821), sin revisión externa o control como requisito para su puesta en funcionamiento, y sin exigir mayores precisiones. Otorgar un formulario amplio para que cada empresa pueda completar como considere en los hechos implica desnaturalizar el estudio previo que se pretende obtener y el gravamen irreparable que puede generar en derechos. Para poder entender el alcance del impacto de la tecnología es indispensable incluir requisitos técnicos precisos e instancias de control independientes sobre los resultados que la propia empresa provea. Esta independencia es, además, un estándar internacional: ahondaremos en este punto en la sección III.

II.b. Los pliegos no garantizan la protección de datos personales ni prevé suficientes controles institucionales

II.b.1. El PBCP habilita a la empresa a reutilizar los datos para entrenar sus propios sistemas de IA.

El último párrafo del art. 63 de la última versión del PBCP dispone que “la información y los datos a los que acceda el adjudicatario no podrán ser reutilizados ni empleados para el entrenamiento, ajuste, validación, desarrollo o mejora de sistemas o modelos de inteligencia artificial sin autorización previa y expresa del MSEG”. Es decir, siempre que exista esa habilitación -discrecional, sin parámetros ni requisitos- quedará habilitado a hacerlo. Vale remarcar que la cláusula no figura en las primeras versiones del pliego que obran en el expediente, sin explicación sobre la inclusión posterior.

Esta autorización es difícil de conciliar con otras cláusulas del mismo PBCP, como el art. 65 que establece que el procesamiento de datos de la empresa se limita a “funciones de mantenimiento y soporte” sobre infraestructura controlada por el Ministerio, y que el contrato de procesamiento de datos debe incluir “la prohibición expresa de utilizar los datos para fines propios o distintos a los instruidos por el MSEG”. **Se debería limitar la procedencia de esa autorización, o directamente eliminar su posibilidad.**

Otro punto problemático de la formulación actual es que, según remarcó el Ministerio en la audiencia judicial, este proceso encuentra fundamento en el art. 15 de los “Lineamientos Operativos” que dice “Cuando los organismos contraten soluciones de IA provistas por terceros, deberán aplicar los presentes lineamientos y contemplar (...) cláusulas sobre finalidad de uso, titularidad y tratamiento de datos, prohibición de entrenamiento o reutilización no autorizada de datos del Gobierno de la Ciudad, confidencialidad, seguridad de la información, ubicación y subprocesamiento de datos, auditoría y trazabilidad, documentación técnica, cambios relevantes, incidentes, continuidad operativa, reversibilidad, portabilidad, interoperabilidad, eliminación o devolución segura de datos, responsabilidades del proveedor y cumplimiento de la normativa vigente”. Sin embargo, esto es conceptualmente inaplicable: los datos biométricos recolectados por estos sistemas **siguen siendo datos personales de cada persona y los titulares del dato son, justamente, ellas mismas**. Es decir que no se trata de “datos del Gobierno de la Ciudad”, en los términos en que está contemplado en los “Lineamientos Operativos” que el Ministerio presentó como fundamento. Si bien las disposiciones allí previstas son valiosas, lo cierto es que no son aplicables al caso concreto por no ser el Gobierno el titular de los datos en cuestión. Así, es indispensable **garantizar de manera expresa dentro del pliego la prohibición de reutilización**, independientemente de esos Lineamientos.

Es que, además, la reutilización se aparta del principio general de “finalidad” que caracteriza el tratamiento de datos personales y que recoge expresamente la Ley 25.326 (art. 4), y sobre el que la Corte Suprema de Justicia de la Nación se pronunció recientemente *in extenso* en el caso Torres Abad³. En la práctica, los datos captados para tareas de seguridad pública, incluidos los rostros de personas bajo búsqueda judicial, podrían terminar alimentando productos comerciales de una empresa privada, sin que esas personas hayan consentido ese uso.

En este escenario, para cumplir con los principios generales de protección de datos y con la propia Ley 25.326 y el mandato de la CSJN, es indispensable: a) limitar la discrecionalidad de la autorización, b) establecer la prohibición de reutilización de los datos por parte de las

³ CSJN, Torres Abad, Carmen c/ EN - JGM s/ hábeas data, sentencia del 30/04/2026.

empresas para cualquier otra finalidad, independientemente de los “Lineamientos Operativos”.

II.b.2. La retención de datos admite una excepción discrecional sin plazo máximo, y los plazos de 60 días no están justificados.

El art. 64 del mismo PBCP dispone que, “cumplidas las tareas encomendadas y entregados los datos al organismo contratante”, el adjudicatario eliminará los datos de forma segura “salvo instrucción expresa del MSEG fundada en una finalidad concreta y por el plazo que éste determine”. Vale mencionar que las versiones anteriores del pliego disponían un plazo máximo de conservación, de 2 años, que fue eliminado. En este escenario, el Ministerio puede prolongar la guarda de datos personales, incluidas imágenes biométricas, sin tope y precisiones sobre qué se entiende por “finalidad concreta”, y/o si cualquier tipo de finalidad es admitida.

Por otra parte, el PET dispone que se resguarden por 60 días corridos aquellos eventos que resulten en alertas positivas “con fines de auditoría”, sin distinguir si se trata de reconocimientos efectivos de una persona o de falsos positivos.

En el primer caso, debería alcanzar con la remisión de la información al juzgado, sin necesidad de almacenarla. En el segundo, pensando en falsos positivos, 60 días parece ser poco tiempo para revisarlo. Debería incorporarse una definición clara frente a qué tipo de eventos puede activarse el almacenamiento, prever un plazo máximo y exigir una justificación adecuada por parte del Gobierno para hacerlo.

II.b.3. No hay mecanismos de revisión humana previstos expresamente

Si bien se declara a lo largo del PET la importancia de las instancias de revisión humana (por ejemplo, las alertas no podrán fundar una actuación susceptible de afectar derechos sin una revisión humana previa, expresa y registrada (art. 3), el sistema debe permitir validar la identificación y registrar el resultado de la revisión humana (art. 4), los registros de auditoría deben permitir reconstruir “el resultado de la revisión humana” (art. 6), entre otras), lo cierto es que no define quién debe hacer la revisión, con qué criterio ni en qué tiempo, ni cómo se verifica que sea sustantiva y no una validación formal, como exige el principio (b) de los “Lineamientos Operativos”. En la audiencia el Ministerio explicó que la alerta pasa por el área de biometría de la policía antes de cualquier detención, pero no consta en el pliego. Se trata de cuestiones que deberían estar establecidas de manera expresa y previa, de forma tal que no se trate únicamente de una voluntad declamativa sin correlato exigible en la práctica.

III. Lineamientos mínimos para una evaluación de impacto en privacidad de sistemas de reconocimiento facial.

En función de todo lo expuesto, consideramos fundamental que se precise el alcance de la Evaluación de Impacto en Privacidad sobre el sistema, incluyendo en qué condiciones se debe realizar y qué contenidos deben medirse.

En este sentido, en función de la *expertise* de Vía Libre en la intersección entre derechos humanos y tecnologías, ofrecemos a continuación algunos puntos que podrían considerarse

“lineamientos mínimos” para guiar cómo debería realizarse una evaluación de impacto de este tipo de tecnologías. Incluimos, también, un primer apartado sobre las exigencias mínimas que debería contemplar un pliego de licitación de este tipo de sistemas para que, una vez contratada la empresa proveedora, su despliegue tenga la posibilidad de ser efectivamente respetuoso de los DDHH.

Se apoyan en los propios “Lineamientos Operativos” (art. 11), en el actual Anexo I del PET, basado en ISO/IEC 29134, en lo discutido en la audiencia y en los principios internacionales que rigen la materia. En este sentido, en particular nos propusimos tomar como guía los Principios sobre uso policial de Reconocimiento Facial de la red INCLO⁴, consensuados entre expertos de organizaciones de la sociedad civil de más de 15 países y de los 5 continentes de distintas trayectorias y áreas de *expertise*, y que, además, remiten a instrumentos del derecho internacional que fijan los máximos estándares en la materia. Nos referiremos, en particular, a aquellos que hacen referencia a la auditabilidad y el impacto en derechos. Resulta importante aclarar que, si bien INCLO aclara expresamente que no avala el uso policial de reconocimiento facial -y tampoco lo hacemos desde FVL en esta presentación-, sí consideramos fundamental que, en caso de llevarse adelante, se haga de acuerdo a pautas claras en consonancia con el derecho internacional de los derechos humanos.

Proponemos los siguientes lineamientos de manera genérica, de modo tal que sirvan como piso/estándar y puedan ser acomodados a las especificidades que el propio GCBA decida, en ejercicio de sus competencias, pretender para este sistema. Permanecemos a disposición de V.S. para profundizar, en sentido técnico y jurídico, aquello que fuera necesario.

III.a. Exigencias mínimas que debería contemplar cualquier pliego de licitación

A continuación presentamos una síntesis de exigencias que responden a las observaciones desarrolladas anteriormente que, consideramos, los pliegos y el contrato deberían contemplar para que un sistema de esta naturaleza pueda ser licitado y operado de acuerdo a estándares de derechos humanos.

Es indispensable su inclusión expresa en ambos documentos, de modo tal que la firma adjudicataria no alegue luego imposibilidades de cumplimiento por diversas razones. A su vez, fijar estos estándares como condiciones de contratación permite a las empresas oferentes prever de forma anticipada si efectivamente van a estar en condición de cumplirlos. Las reglas de juego deben estar claras desde el inicio para todas las partes, tanto para tener claridad en qué se espera como para que la competencia entre los proveedores también sea transparente.

III.a.1. Auditabilidad y control reales. El propio pliego debe definir quién audita (un tercero independiente del proveedor, como veremos más adelante), con qué periodicidad, qué se audita (el modelo, los datos de entrenamiento y el desempeño por subgrupo, no solo los procesos de integración de datos como hoy prevé el PET), con qué acceso (como obligación contractual de la empresa y no como declaración jurada) y qué parte de los resultados se hace pública. La autoridad debe comprender cómo funciona el sistema y el proveedor debe poder explicarlo.

⁴ International Network of Civil Liberties Organizations (INCLO), “Eyes on the Watchers: Challenging the Rise of Police Facial Recognition. Principles to reduce the human rights harms of facial recognition technology”, disponibles en <https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/>.

III.a.2. Ciclo de vida de los datos. Debe fijar la finalidad única, plazos máximos de retención y de destrucción, la prohibición de reutilización para entrenar sistemas de la empresa o, si se admitiera una excepción, los parámetros y requisitos de la autorización, y los flujos de información y autorizaciones entre la empresa y el Gobierno. También debe describir la base de datos de referencia: cómo se obtienen las imágenes, cuánto se conservan, quién accede, cada cuánto se depura, cómo se saca a una persona de ella y con qué criterio se la incluye (ver principio 8 de INCLO).

III.a.3. Contexto de uso y revisión humana. Debe documentar toda la capa de aplicación y no solo la herramienta: protocolos de intervención humana, capacitación, tiempos, registro, auditoría de esa revisión y resoluciones de actuación policial, con un argumento suficiente sobre por qué no habrá detenciones poco razonables (debe exigirse un “*safety assurance case*”, ISO 15026, como explicó el perito experto), lo que requiere incluir información de contexto.

III.a.4. Corrección y mejora continua. Debe prever un circuito de retroalimentación de los falsos positivos para que el sistema no siga identificando mal a la misma persona, monitoreo continuo con revisión de sesgos, la revisión periódica de la propia evaluación y la suspensión o el retiro del sistema si falla una evaluación posterior. Además, debería incluir el aviso a la persona identificada erróneamente y un informe anual público, anonimizado, de las identificaciones erróneas (para más información ver Principios 2, 14 y 15 de INCLO).

III.b. Condiciones en que debe realizarse la evaluación

III.b.1. La evaluación debe tener una instancia independiente de la empresa proveedora. Debe ser realizada, o al menos dirigida y validada, por una entidad sin vínculo económico ni contractual con ningún oferente, con el adjudicatario ni con sus subcontratistas, y no debe apoyarse exclusivamente en las métricas, las pruebas ni los informes que los oferentes producen sobre sus propios sistemas. La evaluación debe ponerse a disposición de un órgano de control independiente antes de la puesta en funcionamiento. Es que el deber de evaluar debe ser “indelegable” para la autoridad estatal, a pesar de que hoy el pliego va en sentido contrario. Proponemos que sean los órganos de control (la comisión de la Legislatura y la Defensoría) quienes designen a las autoridades a cargo de realizar la evaluación.

III.b.2. Previa y actualizada. Debe presentarse y aprobarse antes de adjudicar y antes de procesar cualquier dato real, y no después de la marcha blanca, y debe haber una decisión expresa de aprobación distinta a la voluntad de la empresa. Los propios “Lineamientos Operativos” exigen la evaluación documentada antes de la adquisición, la prueba piloto o la implementación. A su vez, los Principios de INCLO sostienen que la autoridad debería re-evaluar antes de desplegar cualquier uso nuevo y repetirla anualmente (principio 2).

III.b.3. Resultado vinculante. La evaluación debe poder concluir si el sistema debe o no ponerse en funcionamiento, o que solo puede hacerlo si se mitigan determinados riesgos, y ese resultado debe condicionar una autorización independiente. El propio Anexo I hoy prevé las opciones “proceder / proceder con medidas / no proceder” y “proyecto rechazado / suspendido”, pero el PET no les da ningún efecto; este es el punto que se debe corregir. Todo sistema que no supere la evaluación no debe desplegarse. Esto implica la resolución anticipada del contrato con la empresa proveedora si en algún momento del ciclo las evaluaciones (periódicas) no fueran superadas.

III.c. Qué debe medir y documentar la evaluación

III.c.1. Debe ser específica del sistema, no genérica. Es necesario que describa de manera precisa las especificidades técnicas del sistema que se ofrece. En el caso de tecnologías de reconocimiento facial esto incluye, de mínima, analizar:

- los parámetros concretos del uso;
- los derechos afectados (privacidad, protección de datos personales, libertad de expresión y de reunión pacífica, no discriminación);
- la naturaleza y la extensión de los riesgos para esos derechos;
- cómo se mitigará cada riesgo;
- la justificación demostrada de por qué los beneficios superan el impacto sobre los derechos;
- qué remedio tiene quien sea identificado erróneamente, entendido como la selección equivocada de una persona de la lista de candidatos por un revisor humano, previa a una actuación policial, o cuyos datos biométricos se hayan tratado cuando no correspondía

Para más desarrollo sobre este punto, recomendamos la lectura del Principio 2 de INCLO, antes citado.

III.c.2. Evaluación de sesgos e impacto diferencial. Debe documentar el origen, la calidad, las limitaciones, las transformaciones y los riesgos de sesgo de los datos de entrenamiento, incluida la representación demográfica de la población buscada. También medir el desempeño desagregado por grupo poblacional y con validación independiente, y prever una evaluación diferenciada y no solo una tasa agregada. No deberían desplegarse nuevos usos si la evaluación determina que el sistema y la composición demográfica de su conjunto de entrenamiento producen resultados sesgados, directa o indirectamente, contra una característica protegida en un contexto operativo. Este punto podría apoyarse en el programa de normas ISO del INTI que el Ministerio, durante la audiencia, mencionó haber consultado (no tenemos información suficiente para confirmarlo).

III.c.3. Metodología de medición del desempeño. Debe mostrar de manera clara cómo se miden los falsos positivos y los falsos negativos y a qué nivel de ajuste de los umbrales, en qué condiciones de captura (posición de la cámara, colaboración de la persona, contexto de multitud o de persona aislada), con qué criterio de comparación y con qué estándar de referencia. A la vez, debe aclarar si las tasas de error reflejan condiciones de laboratorio u operativas, que reproduzcan la composición demográfica del lugar donde se usará (ver principio 8 de INCLO). De lo contrario, la evaluación es en abstracto y no permite conocer el impacto real.

IV. CONCLUSIÓN

En términos generales, los pliegos no recogen lo que la Justicia ya exigió para el sistema anterior. La Sentencia de Primera Instancia y de Cámara, y la pericia de los expertos de la UBA que reclama un estándar de auditabilidad del tipo "*safety assurance case*" (ISO 15026)⁵, no aparecen siquiera mencionadas en el expediente administrativo de esta licitación, a pesar de que la propia solicitud de contratación de la Comisaría General (SIPGE) presenta el nuevo servicio como de "similares características técnicas" al anterior (tal como se recoge en el dictamen jurídico obrante a partir de p. 663). Únicamente se menciona como antecedente el encendido excepcional del sistema en 2025. El Ministerio manifestó en la audiencia que incorpora los lineamientos de las sentencias pero, como vimos, a pesar de la buena intención muchas cuestiones siguen siendo declamativas y no tienen un correlato concreto en el expediente administrativo.

La licitación aún no fue aprobada ni publicada, por lo que es este el momento de fortalecer los pliegos de modo tal que, una vez adjudicado el sistema, no dependa de la voluntad de la empresa el despliegue de una tecnología respetuosa de derechos. Las deficiencias que señalamos se concentran en tres puntos centrales, que las sentencias ya habían identificado como condiciones del funcionamiento del sistema. Primero, la auditabilidad: el control excluye el motor algorítmico y los datos de entrenamiento, y descansa en una declaración jurada de la propia empresa. Segundo, la evaluación de impacto: es un formulario genérico, a cargo del adjudicatario, que se presenta después de la adjudicación y de la marcha blanca, sin revisión independiente ni efectos sobre la puesta en funcionamiento. Tercero, la protección de datos: se admite su reutilización con una autorización discrecional y se permite una retención sin plazo máximo. Sin una corrección de estos puntos, el sistema que se contrate no podrá ser auditado ni evaluado de manera previa e independiente, y el Tribunal no tendrá cómo verificar el cumplimiento de lo que ordenó.

Así, los pliegos dejan un margen de discrecionalidad tan amplio que no parece verosímil que su implementación cumpla las garantías que declaran, incluso suponiendo las mejores intenciones de cumplimiento y apego a los estándares fijados por la Justicia. Cuando se trata de tecnologías tan intrusivas y de vigilancia masiva, es indispensable fijar reglas rigurosas, verificables y exigibles desde el inicio, y con control independiente durante todo el ciclo. Con ese propósito presentamos estas observaciones y los lineamientos mínimos del apartado III, y solicitamos lo que se detalla a continuación.

V. PETITORIO

Por todo lo expuesto, solicitamos a V.S.:

1. Se tengan por presentadas las observaciones y los puntos mínimos aquí expuestos, en cumplimiento del compromiso asumido en la audiencia del 25/09/2026.
2. Se disponga que los pliegos prevean, como obligaciones contractuales exigibles:
 - a. el acceso a una auditoría independiente sobre el motor algorítmico, los datos de entrenamiento y el desempeño por subgrupo poblacional;

⁵ Para más detalle sobre este procedimiento ver acta de la audiencia del día 03/05/2024, Actuación Nro: 891971/2024.

- b. una evaluación de impacto específica del sistema, previa a la adjudicación y a todo tratamiento de datos reales, realizada o validada por una entidad independiente, con resultado vinculante;
- c. la prohibición expresa de reutilizar los datos para entrenar sistemas de la empresa, y plazos máximos de retención justificados;
- d. la definición de las métricas de error (falsos positivos y negativos, umbrales, condiciones de captura) y su medición desagregada por grupo.

Subsidiariamente, en el caso de que V.S. considerara improcedente este requerimiento, solicitamos se tengan presentes los lineamientos mencionados y se requiera al GCBA que fundamente su eventual apartamiento (si decidiera no incorporarlos).

- 3. Se ordene incorporar a esta causa las resoluciones de actuación policial invocadas por el Ministerio y la documentación técnica del funcionamiento del sistema (arquitectura, flujos de datos y revisión humana).
- 4. Se habilite la participación de los *amicus curiae* de esta causa en las pruebas funcionales, previa autorización del Tribunal.
- 5. Se tenga presente la reserva de ampliar estas observaciones ante cualquier modificación de los pliegos en cuestión.

Proveer de conformidad,

ES DERECHO