

SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS: DOS PUNTOS CIEGOS DESDE LA ÓPTICA DEL DERECHO ADMINISTRATIVO¹

Romina N. Costa²

1. INTRODUCCIÓN

Este trabajo tiene por objeto analizar el fallo *“Observatorio de Derecho Informático Argentino O.D.I.A. y otros contra GCBA sobre amparo – otros”*³, dictado el 28/04/2023.

Dicha sentencia reviste interés desde tres aspectos: por un lado, en relación con la posible afectación a determinados derechos humanos; y, por otro lado, en lo que atañe a los “puntos ciegos” que escapan al desarrollo del pronunciamiento bajo análisis. En torno a esta última cuestión, concretamente, nos referimos al procedimiento de contratación del software utilizado para implementar el Sistema de Reconocimiento Facial de Prófundos – en adelante SRFP– en la Ciudad Autónoma de Buenos Aires –en adelante, CABA–, y a los secretos profesionales derivados de la propiedad intelectual.

En ese sentido, en las líneas que siguen reflexionaremos sobre las tensiones entre los derechos de la ciudadanía, las facultades del Gobierno de la Ciudad Autónoma de Buenos Aires –en adelante, GCABA– para contratar como lo hizo, y la posibilidad de obtener una declaración testimonial donde se intersecan secretos profesionales e interés público.

2. LOS HECHOS DEL CASO

El Observatorio de Derecho Informático Argentino –en adelante, ODIA– promovió una acción de amparo contra el GCABA por entender que se encontraban afectados derechos

¹ Cítese como Costa, R. 2023. Sistema de Reconocimiento Facial de Prófundos: dos puntos ciegos desde la óptica del derecho administrativo, Estudios sobre Jurisprudencia, 328-350.

² Abogada (UBA) y Profesora para la Enseñanza Media y Superior en Ciencias Jurídicas, distinguida con diploma de honor Maestranda en Derecho Administrativo y Administración Pública, tesis presentada a la espera de designación de jurado (UBA). Ayudante de Primera *ad honorem* en “Elementos de Derecho Administrativo” (UBA). Auxiliar en el Consejo de la Magistratura de la CABA.

³ Cám.CATyRC, Sala I, “Observatorio de Derecho Informático Argentino O.D.I.A. y otros contra GCBA sobre amparo – otros”, Expediente N° 182908/2020-0, sentencia del 28/04/2023. Esa decisión y las restantes que tuvieron lugar en el marco de ese proceso, están recopiladas y resumidas en el boletín *“La judicialización de los Sistemas de Reconocimiento Facial”* elaborado por la Escuela de la defensa pública del MPD junto al Observatorio de Derecho Informático Argentino (O.D.I.A.)

fundamentales a través de la Resolución N°398/MJYSGC/19⁴ y la Ley N° 6339⁵ –que modificó la Ley N° 5688⁶ en sus arts. 478⁷, 480⁸, 484⁹, 490¹⁰ e incorporó los arts. 480 bis¹¹

⁴ Esta norma (previa a la vigencia de la Ley N° 6339, y que fue declarada no vigente por la Ley N° 6588, sancionada el 10/11/2022 y publicada el 12/12/2022 en el BOCABA N° 6517) aprobó la implementación en el ámbito de la CABA del SRFP (art. 1°), cuya operación y funcionamiento quedaba sujeto a lo dispuesto en el IF-2019-12925085-GCABAMJYSGC que la integra (Anexo). Asimismo, facultó a la Secretaría de Justicia y Seguridad del Ministerio de Justicia y Seguridad local –en adelante, MJyS– a dictar las normas complementarias, operativas y aclaratorias que resulten necesarias y pertinentes para la efectiva implementación de este sistema (art. 2°). Además, invitó a la Defensoría del Pueblo de la CABA a auditar el funcionamiento del SRFP, instruyendo a la citada Secretaría a gestionar la suscripción del pertinente convenio entre ambos organismos, dentro del plazo de treinta (30) días (art. 3°). Su Anexo (IF-2019-12925085-GCABA-MJYSGC) dispone que el mentado sistema opera por intermedio del Sistema Público Integral de Video Vigilancia –en adelante, SPIVV– de la CABA previsto en la Ley N° 5688, respetando los ejes fundamentales y principios rectores plasmados en esa norma (art. 1°). Limita su empleo únicamente para tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial de la Nación, Provincial y de la CABA, 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 –en adelante, CONARC–. Prohíbe incorporar imágenes y registros de otras personas que no se encuentren registradas en la CONARC, salvo orden judicial que lo habilite (art. 2°). En su art. 3° explica que esta herramienta se integra con la totalidad de los registros incorporados en la CONARC y con los datos biométricos consultados del Registro Nacional de las Personas –en adelante, RENAPER–, debiendo corresponder estos últimos única y exclusivamente a personas que registren orden judicial de restricción de la libertad registradas en la base de la CONARC. Este requerimiento deberá ser dirigido a la Secretaría de Justicia y Seguridad. A la vez, impone el deber de confidencialidad al personal autorizado para la operación y acceso al SRFP por el MJyS, mediante la suscripción del convenio respectivo (art. 4°). Determina que todo archivo generado a partir del uso del SRFP debe quedar en poder de la autoridad policial y, a su respecto, se aplicarán los protocolos de seguridad, privacidad y confidencialidad. Castiga la difusión no autorizada mediante la aplicación del régimen disciplinario de la Ley N° 5688, sin perjuicio de las sanciones civiles y penales que pudieran corresponder (art. 5°). Establece que la operación del SRFP está a cargo del Centro de Monitoreo Urbano –en adelante, CMU– de la Policía de la CABA. Detalla que cuando el sistema detecta una coincidencia, el CMU genera una carta de servicio y da aviso al personal policial de acuerdo con los protocolos vigentes (art. 7°). Dispone que, una vez cumplida la orden judicial de restricción de la libertad, o que la misma haya cesado, los datos personales tratados deberán ser destruidos (art. 8°), de acuerdo con los principios que emanan de la normativa, local y nacional en la materia.

⁵ Sancionada el 22/10/2020 y publicada el 19/11/2020 en el BOCABA N° 6002, luego fue declarada no vigente por la Ley N° 6588, sancionada el 10/11/2022 y publicada el 12/12/2022 en el BOCABA N° 6517.

⁶ Su art. 474 creó el SPIVV de la CABA. El art. 475 establece que la utilización por parte del Poder Ejecutivo de los sistemas de video vigilancia destinados a grabar imágenes en lugares públicos y a los que se refieren los arts. 485 y 486, estableciendo específicamente el posterior tratamiento de tales imágenes y el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente en las sucesivas fases de grabación y uso de las imágenes. A la vez, el art. 476 dispone que su uso está regido por los principios de proporcionalidad y razonabilidad en su doble versión de procedencia y de intervención mínima, y que la procedencia determina que sólo podrá emplearse cuando resulte adecuado, en una situación concreta, para asegurar la convivencia ciudadana, la utilización pacífica de las vías y espacios públicos, la elaboración de políticas públicas de planificación urbana, así como para la prevención de faltas, contravenciones y delitos y otras infracciones relacionadas con la seguridad pública; mientras que la intervención mínima exige la ponderación en cada caso de la finalidad pretendida y la posible afectación al derecho a la propia imagen, a la intimidad y a la privacidad de las personas, de

y 490 bis¹²—, por concebir a dicho acto y tales modificaciones como inconstitucionales y contrarias a los distintos Convenios Internacionales firmados por el país. Tales cuestiones se vinculaban al SRFP, el Sistema Preventivo y el Sistema Forense, sus correspondientes Registros de Base de Datos Informatizada y en las que se realizaban tratamientos de datos automatizados, el sistema de borrado o conservación de imágenes y videos, los plazos para remitir informaciones, modificaciones y criterios en cuanto a la implementación del SRFP. También cuestionó que no existieron informes previos a poner en marcha el sistema, y que al interponer la acción no estaba conformada la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia, en la Legislatura de la CABA y no se permitía que ella o la Defensoría del Pueblo local realizaran controles sobre el acto administrativo y las leyes cuestionadas.

En definitiva, ODIA destacó que perseguía la tutela jurisdiccional de los derechos de la sociedad frente a la presunta conducta ilegítima y arbitraria del GCABA, por entender afectados los derechos consagrados en los arts. 14, 14 bis 18, 19, 33, 43, 75 inc. 22 de la

conformidad con los principios consagrados en la Constitución Nacional —en adelante CN— y la Constitución de la Ciudad Autónoma de Buenos Aires —en adelante, CCABA—.

A la par, el art. 477 establece los principios rectores a los que está sujeta la gestión del SPIVV.

⁷ Prevé que la instalación de sistemas de video vigilancia por parte del Poder Ejecutivo procede en la medida en que resulte de utilidad concreta a fin de proporcionar información necesaria para adoptar eventuales medidas de gobierno relacionadas con la utilización del espacio público, para lo cual es necesario tener en cuenta una distribución territorial equitativa en función de las situaciones cuyo objetivo se busca atender y contemplarse al Mapa del Delito como herramienta para su instalación.

⁸ Determina que “[l]as referencias a sistemas de video vigilancia, se entienden hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en este Libro, como así también al Sistema de Reconocimiento Facial de Prófundos, al Sistema Preventivo y al Sistema Forense”. Esa misma regla prevé que el SRFP tiene como objetivo la identificación y el reconocimiento de personas prófugas de la justicia basado en el análisis en tiempo real de imágenes de video.

⁹ El sistema establece que las grabaciones son destruidas una vez transcurridos sesenta (60) días corridos desde su captación, salvo las que estuvieran relacionadas con infracciones penales o administrativas en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

¹⁰ La autoridad de aplicación del SPIVV de la CABA tiene a su cargo la creación de un Registro en el que figuren todos los sistemas de video vigilancia comprendidos en el art. 480, especificando su estado operativo y otros datos que puedan resultar de interés.

¹¹ Este artículo disponía que el SRFP sería empleado únicamente para tareas requeridas por el Poder Judicial de la Nación, Provincial y de la CABA, como así también para detección de personas buscadas exclusivamente por orden judicial, registradas en la CONARC. Salvo orden judicial, se encuentra prohibido incorporar imágenes, datos biométricos y/o registros de personas que no se encuentren registradas en la CONARC.

¹² Estatuyó en el ámbito de la Legislatura de la CABA la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia, integrada por los presidentes de las Comisiones de Justicia y de Seguridad, y tres diputados designados por la Vicepresidencia Primera del cuerpo, con facultades para convocar a especialistas y organizaciones de la sociedad civil para analizar y proponer sobre los aspectos que son de su incumbencia.

CN; los arts.14, 16, 18, 34, 36, 38, 39, 61 de la CCABA; la Opinión Consultiva N° 5/85 de la CIDH (derecho a reunión de terceros); el art. 1710 del Código Civil y Comercial de la Nación; y el art. 7º del Pacto de San José de Costa Rica, entre otros.

Asimismo, resaltó que la aplicación de este tipo de sistemas en otras partes del mundo había sido precedida de amplios debates por parte de la ciudadanía y las autoridades y que más allá de que –en algunos casos– su uso había resultado justificable y en otros cuestionable, donde se terminó adoptando el sistema, su justificación, legitimidad, necesidad y proporcionalidad se había establecido mediante una evaluación del impacto en la privacidad –en adelante, EIP–. Añadió que el GCABA no realizó esa EIP.

Por otro lado, señaló que –con anterioridad a la promoción del amparo bajo estudio– había iniciado otra acción¹³ con el fin de que el GCABA le brindase toda la información relacionada con la Resolución N° 398/MJySGC/2019, dado que el pedido formal que había planteado en sede administrativa había sido respondido de manera parcial.

3. PERIPLO DEL PROCESO HASTA CULMINAR EN EL DICTADO DE LA SALA I DE LA CÁMARA DE APELACIONES EN LO CONTENCIOSO ADMINISTRATIVO, TRIBUTARIO Y DE RELACIONES DE CONSUMO

3.1. Aclaraciones preliminares

Previo a discurrir sobre los términos de la sentencia de la Sala, cabe formular ciertas consideraciones acerca del devenir del proceso que derivó en el dictado del fallo que nos ocupa y que revelan sendas aristas interesantes. Así, cabe decir que en el marco de este proceso se requirió una medida cautelar, se registraron varias recusaciones a los titulares a cargo de los juzgados de primera instancia, se presentaron diversas personas para intervenir como *amicus curiae*¹⁴ y otras para obrar como partes¹⁵, se tomó una audiencia testimonial en la cual un testigo sostuvo no poder responder a ciertas preguntas del tribunal porque violaría un convenio de confidencialidad firmado con su empleador.

¹³ Dicha acción quedó radicada en el Juzgado de Primera Instancia en lo CATyRC N° 23, Secretaría N° 45, bajo el Expediente N° 9480/2019-0. Dicho proceso fue favorablemente acogido en primera instancia. Luego, la Sala III de la Cám.CATyRC, en fecha 19/03/2021, rechazó las apelaciones interpuestas, y confirmó la sentencia de grado, con imposición de costas de la instancia al GCABA vencido. Ello originó que éste interpusiera recurso de inconstitucionalidad, el que fue rechazado en fecha 25/12/2021 por la Sala III del fuero, con imposición de costas a la recurrente vencida.

¹⁴ Como *amicus curiae* se presentaron: Asociación de Trabajadores del Estado (ATE), Coordinadora contra la Represión Policial e Institucional (CORREPI), Organización No Gubernamental de Desarrollo, Defensa y Promoción de los Derechos Humanos en el Entorno Digital (“Derechos Digitales”), Gaspar Pinasu (Líder de Políticas Públicas para América Latina de la Organización Internacional de Derechos Humanos “Access Now” y Fundación Vía Libre. Su petición fue aceptada por el tribunal de primera instancia.

¹⁵ Dedujeron amparo y adhirieron al presente litigio Paula Castillejo Arias y Víctor Leopoldo Castillejo Rivero, fundando su legitimación en calidad de habitantes. Asimismo, el Centro de Estudio Legales y Sociales (CELS) solicitó intervenir como parte actora.

3.2. Dictamen del Ministerio Público Fiscal de primera instancia

Previo al dictado de la sentencia interlocutoria, el juzgado de grado dio intervención al Ministerio Público Fiscal (Unidad Especializada en Litigios Complejos), quien emitió su dictamen¹⁶. Allí sostuvo que

[L]a normativa [...] aborda el tratamiento que debe otorgársele tanto a la información obtenida por las cámaras de videovigilancia como a la que surge de la Consulta Nacional de Rebeldía y Capturas, previendo las consecuencias disciplinarias y penales que tendrán quienes tengan acceso y no cumplan con las disposiciones específicamente contempladas, así como un plazo razonable para su destrucción. [S]u utilización no resultaría desproporcionada o irrazonable teniendo en miras las misiones asignadas a las fuerzas de seguridad locales relativas a la detención de personas prófugas de la justicia con la finalidad de disminuir la delincuencia en el ámbito de la ciudad y, asimismo, colaborar con los requerimientos de las distintas jurisdicciones.

Por otro lado, en cuanto a la afectación de los derechos de intimidad y de reunión, señaló que

ni las alegaciones de las partes ni las pruebas arrojadas a la causa tendrían la suficiente entidad como para tenerla por configurada. Sin soslayar que las partes accionantes alegan la falta de concreción de la Evaluación de Impacto a la Privacidad (EIP), de modo previo a la implementación del proyecto criticado, no se encontraría acreditado una circunstancia específica en la que el derecho a la intimidad de los habitantes de la ciudad haya sido afectado, ni tampoco que dicha afectación pueda deducirse automáticamente a partir de las características inherentes del sistema.

Finalmente, sostuvo que “la falta de material probatorio que dé cuenta de una eventual afectación al derecho a la no discriminación sellaría la suerte de su reconocimiento”.

3.3. Sentencia interlocutoria de primera instancia

El juez de grado dictó una serie de medidas para mejor proveer¹⁷ y, posteriormente, dictó sentencia¹⁸ por la que hizo lugar a la medida cautelar, a través de la cual suspendió la aplicación del SRFP en el ámbito de la CABA, sin que ello mermase los restantes sistemas de videovigilancia (monitoreo urbano), preventivo y forense. A la par, hizo saber a la ciudadanía que el resolutorio no implicaba un menoscabo en el servicio de seguridad

¹⁶ Actuación N° 2.363.828/2021, de fecha 25/10/2021.

¹⁷ Actuación N° 2.384.543/2021, de fecha 27/10/2021.

¹⁸ Actuación N° 783.420/2022, de fecha 11/04/2022.

pública, dado que SRFP se encontraba inactivo por decisión del Poder Ejecutivo local y que lo decidido no alteraba los sistemas vigentes de videovigilancia¹⁹.

Para así decidir, el magistrado sostuvo que *“se puso en marcha el SRFP sin garantizar que este c[ontara] con los organismos de control que el cuerpo legal requ[ería], lo que se da[ba] de bruces con el principio de legalidad que deb[ía] regir todo accionar de la Administración”*.

Añadió que, de acuerdo con la Ley N° 1845²⁰ de Protección de Datos Personales y su Decreto reglamentario N° 725/2007²¹, era obligatorio para el responsable de cada base que contuviera datos personales, inscribirlo en el Registro que funcionaba en el Centro de Protección de Datos Personales, resaltando que la Defensoría del Pueblo local había advertido que las *“bases de datos relativas a videovigilancia y sistema de reconocimiento facial [...] no se enc[ontraban] inscriptos en [su] Registro”*.

A su vez, ponderó que el director del Registro Nacional de Reincidencia –en adelante, RNR–, donde funciona la CONARC²², destacó que *“la utilización de esta base de datos p[odía] motivar algún tipo de conflicto al dar lugar a una detención errónea comúnmente denominada ‘falso positivo’”*, apreciación que coincidió con la volcada por la Defensoría del Pueblo de la CABA en el informe remitido a la Legislatura durante el procedimiento de sanción de la Ley N° 6339.

Luego, hizo referencia a la Evaluación de Impacto en la Protección de Datos (EIPD), a la que apuntó como *“la herramienta más atinada y fundamental a fin de abordar los efectos que la implementación del SRFP [...] pu[diera] tener sobre los derechos humanos de quienes, en este caso, transita[ban] la CABA”*. Sostuvo que, pese a declarar el GCABA que había llevado a cabo pruebas para reducir al máximo posible la tasa de error, no había precisado cuáles habían sido las medidas ejecutadas.

A continuación, aludió a la participación ciudadana como principio rector reconocido en el Sistema Integral de Seguridad Pública de la CABA. Recordó que el art. 495 bis de la Ley N° 5688 creó la aludida Comisión Especial de Seguimiento de los Sistema de Video Vigilancia, donde también podría convocarse a especialistas y organizaciones de la sociedad civil para analizar y proponer aspectos que fueran de su incumbencia, pero que aquella tampoco había sido conformada.

¹⁹ Punto 3°, apartado H).

²⁰ Sancionada el 24/11/2005 y publicada el 03/08/2006 en el BOCABA N° 2494.

²¹ Emitido el 18/05/2007 y publicado el 24/05/2007 en el BOCABA N° 2691.

²² La CONARC es una base de datos pública dependiente del Ministerio de Justicia y Derechos Humanos de la Nación donde la Justicia Federal, Nacional, de la CABA y Provinciales, vuelcan los pedidos de captura sobre personas que han delinquido y se encuentran prófugas.

Seguidamente, describió los derechos que se hallarían afectados: la presunción de inocencia, los derechos personalísimos a la intimidad, honor, imagen, identidad y privacidad, principio de transparencia, y a los derechos a la información y a la participación ciudadana.

Más adelante, el magistrado observó que –conforme el listado provisto por el Ministerio de Justicia y Derechos Humanos de la Nación, las personas incluidas en la CONARC eran treinta y cinco mil (35.000) al 25/04/2019 y al contestar el oficio, ascendían aproximadamente a cuarenta mil (40.000), siendo que las solicitudes de datos biométricos efectuadas por el GCABA entre el 25/04/2019 y el 20/12/2021 ascendieron a nueve millones trescientos noventa y dos mil trescientos setenta y dos (9.392.372); y, entre esta última fecha y el 09/03/2022, alcanzaron la cifra de quinientos siete mil novecientos once (507.911). Resaltó que —en dichos lapsos— el sistema había estado mayormente inactivo y puso de relieve que no se advertían razones que justificaran el acceso a datos personales de individuos que estuvieran fuera de la CONARC, considerando que la cuantiosa migración de datos biométricos tampoco podría obedecer a consultas policiales de operativos de seguridad o de siniestros en la vía pública.

Finalmente, el juez de grado se expidió sobre la medida para mejor proveer reclamada por el CELS y los coactores Paula Castillejo Arias y Víctor Leopoldo Castillejo Rivero, concediéndola en el apartado 4 a 7, con los alcances allí establecidos²³.

²³ En concreto, mediante los puntos 4 a 7 de la sentencia se dispuso lo siguiente:

4º) Ordenar en los términos del art. 29 del CCAyT al Director Nacional de la Policía de Seguridad Aeroportuaria, que por intermedio del cuerpo que dirige: a) el día 12/04/2022, a las 14:00 horas, se presente en las sedes del CMU de la Policía de la CABA y del MJyS del GCABA y secuestre mediante extracción toda la información contenida en la arquitectura informática utilizada en el SRFP—se trate de software propio del GCABA o de terceros—, debiendo retirar en caso de ser necesario los equipos físicos donde aquélla se encuentre contenida; contando para ello con facultades de allanamiento si fuera menester; b) individualizar, en su caso, la presencia del Ministro de Justicia y Seguridad de la CABA, Dr. Marcelo Silvio D'Alessandro; y/o del Subsecretario en Tecnología e Informática, Gastón Leopoldo Navarro; y/o de la Coordinadora del Plan Integral de Videovigilancia de la CABA, Cecilia Inés Amigo; y/o de la Jefa del Departamento de Monitoreo, Comisario Inspector Raquel Cesanelli; y/o de la Jefa de la División Extracción y Análisis de Imágenes, Comisario Laura Malventano; y/o del Jefe de la División CMU, Comisario Damián Fecit; y obtenga de éstas las contraseñas necesarias para ingresar a las bases de datos a extraer. En caso de que tales personas afirmen no poseer tales claves, requiéraseles que sean individualizadas las personas que sí las poseen y obténgase de éstas la información en cuestión; c) inmediatamente al arribo a los inmuebles, deberá apostar una guardia en cada ingreso/egreso, peatonal o vehicular, que verifique mediante identificación cada movimiento de salida y en caso de que se detectare que se trata de alguna de las personas mencionadas se proceda conforme el punto anterior; d) asigne como máximo tres (3) agentes que detentarán tales claves, importando ello un acuerdo de confidencialidad y reserva de las mismas, encontrándose limitado su uso al estricto cumplimiento de la pericia que se ordenará; e) realizar copias de toda la información secuestrada en discos externos, cumpliendo con todos los protocolos de seguridad previstos y asegurando la ininterrupción de los restantes sistemas de monitoreo urbano – videovigilancia forense y preventiva—; f) verificar, una vez concluido el secuestro de la información en

El decisorio fue recurrido por el GCABA en cuanto, por un lado, suspendió el SRFP; y, por el otro, dispuso allanamientos en las oficinas del CMU y el MJyS local con el fin de secuestrar toda la información contenida en la arquitectura informática utilizada en el SRFP. A la vez, la Fiscal a cargo de la Unidad Especializada de Litigios Complejos apeló los puntos 1, 2 y 3 de la parte resolutive y dedujo incidente de nulidad contra los mismos puntos. El juez rechazó el planteo de nulidad y la reposición, y elevó la incidencia a la Sala

cuestión y del equipamiento técnico necesario, la correcta función de los restantes sistemas de monitoreo urbano –videovigilancia forense y preventiva–. A la par, se constituye a la Policía de Seguridad Aeroportuaria como depositaria de la información obtenida en el procedimiento, la que deberá reservarse informando a este Tribunal su ubicación física; g) constituya una consigna de seguridad en la sede de este Tribunal desde el día martes 12/04/2022 a las 12:00, con un móvil a disposición, hasta orden de cese; h) ante la eventual reticencia de las autoridades locales en cumplir con lo solicitado y la posible configuración de delito en los términos del art. 239 del CP, despliegue todas las acciones necesarias y protocolos vigentes en el marco de sus competencias para vencer tal obstáculo. Se hace saber a la Policía de Seguridad Aeroportuaria que ante cualquier consulta que deba realizar al Tribunal, será al juez por conducto de los funcionarios judiciales que se designarán como presentes en la diligencia. A tales fines, líbrense por Secretaría oficio de estilo junto con los mandamientos de rigor, todo ello con habilitación de días y horas inhábiles, vía correo electrónico. Asimismo, se instruye a la secretaria, Dra. Beatriz Campos y al Secretario, Dr. Juan Manuel Nuñez, junto con quienes designen, a constituirse como contralores de la medida en cuestión y a videofilmar íntegramente el procedimiento, a cuyo fin líbrense por Secretaría mandamientos de estilo con habilitación de días y horas inhábiles.

5º) Ordenar en los términos del art. 29 del CCyT a la Policía de Seguridad Aeroportuaria llevar a cabo una pericia informática confiriendo para ello el plazo de diez (10) días a fin de elaborar un informe que pormenorizadamente dé cuenta de los siguientes puntos: a) detalle todas las extracciones realizadas por el MJyS de la CABA y/o la Policía de la CABA, sobre la base de datos biométricos del RENAPER desde el 25/04/2019 al día de la fecha de la pericia; b) realice una comparativa entre los listados de la CONARC, del RENAPER y la información obtenida e indique diferencias cuantitativas y cualitativas, cantidad de coincidencias de registros y cualquiera discordancia que adviertan; c) indique si los datos biométricos obtenidos fueron ingresados o ejecutados en el SRFP y en dicho caso, en qué fecha, su motivo y por orden de quién; d) precise quiénes accedieron a tales datos, con identificación de usuario (nombre, apellido, cargo, función, dirección IP, tipo de acceso o autorización, etc.) con diferenciación de quienes los solicitaron, recibieron, emitieron, reenviaron o manipularon y en el marco de qué orden o procedimiento; e) determine qué tratamiento se le dio a los datos migrados y si fueron eliminados. En tal caso, cuánto tiempo pasó desde que los recibieron hasta que fueron eliminados y qué usuarios realizaron tales acciones; f) informe qué contienen específicamente los datos que migraron desde el RENAPER al MJyS de la CABA y en qué formato se los remitieron; g) aclare si se hicieron pedidos de datos biométricos de personas puntuales o que no se encuentran incluidas en la base de datos de la CONARC, en cuyo caso, identifique cuáles fueron por pedido manual y cuáles por un medio automatizado detallando usuario solicitante; h) dictamine si se ha creado en el ámbito gubernamental local un banco de datos biométricos con los datos migrados desde el RENAPER hacia el GCABA; i) detecte la existencia de videofilaciones almacenadas vinculadas con los datos biométricos migrados, precise las fechas y ponga ellas a disposición del Tribunal; j) detalle si el SRFP estuvo operativo o no, desde el 24/04/2019 hasta el día de la fecha –11/04/2022–, con precisión de si se verifican interrupciones o suspensiones en tal período; k) todo otro dato de interés a la presente causa.

6º) Establecer la reserva de dicha decisión hasta tanto se concretasen las medidas ordenadas.

7º) Disponer la publicación de dicha resolución a través del servicio IJUDICIAL, encomendándole su difusión, a cuyo fin debía remitirse correo electrónico por Secretaría.

l que –previo a dar intervención al Ministerio Público– desestimó los planteos de los apelantes.

Luego, el 11/04/2022 el magistrado de primera instancia corrió traslado de la demanda. Posteriormente, tuvo por presentados a diversos afectados²⁴.

El GCBA dedujo un segundo planteo recusatorio contra el magistrado de primera instancia con motivo de la decisión cautelar adoptada, que fue desestimado por la Alzada.

3.4. Contestación de demanda del GCBA

En lo que atañe a la cuestión nodal de su contestación, el GCBA se explayó sobre la naturaleza del SRFP. Señaló que su objetivo era la “identificación y el reconocimiento de personas buscadas por la justicia basado en el análisis en tiempo real de imágenes de video”, y que “[a]nte la identificación de un rostro perteneciente al grupo de búsqueda, el sistema emit[ía] una alerta, entregando como resultado información sobre la coincidencia según los parámetros de similitud seteados y detalles del origen de la búsqueda (causa judicial)”. Subrayó que las imágenes son capturadas por los dispositivos de videovigilancia y la información obtenida desde su origen hasta el CMU es transportada en forma encriptada mediante el protocolo AES-256. La información de identificaciones que realiza incluye el “time stamp”; dispositivo de captura, recorte del rostro identificado, recorte del rostro del enrolamiento e información de la causa. Aquella se guarda en un repositorio de datos que se encuentra en la sala cofre del MJyS, a la que sólo tienen acceso los usuarios del sistema con privilegios suficientes.

Aclaró que el sistema no almacenaba imágenes de lecturas realizadas, salvo que fueran positivas por coincidir con una persona que se encontraba en la base de datos de la CONARC impartida por la justicia y/u oficio judicial. Reiteró que el SRFP reconoce los rostros de las personas registradas y cotejadas con registros provenientes de la CONARC perteneciente al RNR y/o requerimientos judiciales remitidos.

Explicó que desde el mes de septiembre no se habían registrado errores originados por falsos positivos “*asegurando un accionar certero y preciso en cada oportunidad*”. Advirtió que, al analizar datos biométricos y no simples parecidos, no había umbral de error de identificación, y que la detención, además, no era inmediata, pues se reconocía a la persona, se validaba su identidad y, en caso positivo, se hacía la consulta *in situ* al juzgado interventor que daba las pertinentes instrucciones.

Señaló que el GCABA contribuyó a reducir el margen de error que acarrearía la carga deficiente o desactualizada de la CONARC mediante la depuración de los registros allí contenidos. Insistió que, a partir de septiembre de 2019, debido a la implementación de

²⁴ Myriam Bregman, Nicolás del Caño y Juan Grabois.

optimizaciones tecnológicas no se habían registrados falsos positivos y que las personas aprehendidas en forma equívoca fueron consecuencia de yerros en la carga en la CONARC. A la par, aseveró que no se advertía *“peligro potencial ni real contra las libertades públicas, la libre circulación, la intimidad ni los datos personales que de manera dogmática e infundada el amparista sup[uso] ver vulnerados”*.

Especificó que la transferencia de información entre el RENAPER y el GCABA operaba sobre datos personales y la imagen calificaba como tal; pero para que esa fotografía del rostro constituyera en un dato biométrico era necesario el uso del software especial de reconocimiento facial. Observó que el RENAPER no remitía datos biométricos de ninguna persona, solo la fotografía asociada a un DNI que luego era objeto de un tratamiento técnico con la finalidad de identificar y aprehender personas requeridas por el Poder Judicial.

Concluyó que sobre esa pequeña fracción de datos trataba la presente acción y respecto de ella se extendía la potestad judicial. Destacó, además, que el sistema fue homologado por la firma alemana TÜV Rheinland con norma ISO 9001:2015.

Luego, manifestó que la actora incurría en un error conceptual al extrapolar los números de aprehensiones y de alertas, estableciendo una relación causal directa entre unos y otros. Asimismo, aseguró que el SRFP ya no estaba en proceso de aprendizaje, pues había superado el entrenamiento inicial y solamente contrastaba la información que venía de la CONARC, con el dato biométrico de los prófugos contenido en dicha base de datos, extraídos del RENAPER. A la vez, especificó que el SRFP no estaba entrenado para identificar determinadas etnias sino para buscar similitudes con 562 puntos de reconocimiento facial, comparando un rostro dado con uno en tiempo real.

Finalmente, consideró que de hacerse lugar a la demanda se invadiría la *zona de reserva* de la Administración. Para ello hizo hincapié en que el poder de policía de seguridad pública era una típica función administrativa.

3.5. Sentencia definitiva de primera instancia

Luego de múltiples contingencias procesales, dictaminó el Ministerio Público Fiscal, quien en cuanto a la cuestión de fondo dijo que, a partir del marco probatorio analizado, no se veían afectados los derechos de reunión y a la no discriminación por uso del SRFP, que no existía riesgo de detenciones arbitrarias a ese entonces y que la Evaluación de Impacto a la Privacidad (EIP) –aun cuando fuera reconocida como una buena práctica por el ordenamiento internacional–, por no estar prevista en una norma, no era exigible.

Tras ello, fue dictada la sentencia definitiva de primera instancia que hizo lugar a la acción de amparo. Allí se resolvió: 1) declarar la inconstitucionalidad del art. 1° de la Resolución N° 398/2019 en cuanto el SRFP se implementó sin cumplir los recaudos legales de

protección de los derechos personalísimos de los habitantes de la CABA; 2) disponer la nulidad de todo lo actuado por el MJyS local, en el marco del SRFP, en violación al art. 3° del Anexo de la aludida Resolución (es decir, sin orden judicial constatable); y 3) supeditar la puesta en funcionamiento del SRFP a la constitución y debido funcionamiento de la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia en el ámbito de la Legislatura de la CABA y de la Defensoría del Pueblo local.

Entre los fundamentos esbozados, dijo que el problema no se centraba en el SRFP en sí mismo, sino en las consecuencias que acarrearía su prematura implementación y su utilización en condiciones precarias de respeto por los derechos y garantías de las personas. Para que volviera a ser implementado debía contar con los mecanismos de control, estar incluido en el registro de datos relativo al sistema de video vigilancia, realizar el estudio previo de impacto sobre los datos personales y convocarse a la ciudadanía a debatir sobre dicho mecanismo.

El decisorio fue apelado por Paula Castillejo Arias, Víctor Leopoldo Castillejo Rivero, el CELS, la Unidad Especializada en Litigios Complejos del Ministerio Público Fiscal, ODIA y el GCBA, cuyos recursos fueron sustanciados.

3.6. Sentencia definitiva de la Sala I CATyRC

La sentencia definitiva de este tribunal resolvió rechazar los recursos interpuestos por el Ministerio Público Fiscal, el GCBA, los coactores ODIA, Paula Castillejo Arias y Víctor Leopoldo Castillejo Rivero, y hacer lugar parcialmente a los agravios del coactor CELS.

En consecuencia, ordenó: 1) la rehabilitación del funcionamiento del SRFP, quedando supeditada a la constitución y debido funcionamiento de los órganos de control, y también sujeta 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 GCABA o de quien éste considere adecuado), para determinar si su empleo tiene un impacto diferenciado según las características personales de los individuos afectados; y, 2) antes de poner en funcionamiento el SRFP, se dé a publicidad y se informe –en el ámbito de los FOSEP y a través de la Coordinación– a los vecinos y organizaciones que así lo soliciten la existencia de esta herramienta, su funcionamiento y las reglas jurídicas que en su totalidad lo rigen, a fin de que expongan las observaciones que entiendan necesarias; escrutinios que deberán ser transmitidos a la autoridad de aplicación del SRFP a fin de que exponga las explicaciones necesarias y, de entenderlo procedente, adopte medidas que perfeccionen el sistema.

Para así decir, el tribunal –por unanimidad– consideró, entre otras cuestiones, que el GCABA no contrarrestó las conclusiones a las que arribó la *a quo* sobre la base de la prueba producida. En efecto, no desacreditó que “se puso en marcha el SRFP sin

garantizar que este c[ontara] con los organismos de control que el cuerpo legal tanto nacional como internacional requieren, lo que se da[ba] de bruces con el principio de legalidad que deb[ía] regir todo accionar de la Administración”.

Por otra parte, estimó que el GCABA nada dijo en torno a que la Defensoría del Pueblo local se hallaba imposibilitada de ejercer sus competencias de control según el art. 22 de la Ley N° 1845 y sus funciones²⁵ como auditora del SRPF al no tener a su disposición la información sobre los resultados de gestión del sistema que la autoridad de aplicación está obligada a recabar, analizar y remitirle conforme lo estipulado en el art. 495 de la Ley N° 5688.

A la vez, valoró que el GCABA tampoco refutó que el MJyS local no llevó a cabo un control interno del sistema ni justificó los motivos por los cuales sería suficiente haber limitado la auditoría a la desarrollada por la Universidad de La Plata en el marco del Convenio adjuntado a la contestación de la demanda, cuyas conclusiones no era posible corroborar por no haber acompañado el informe final comprometido en la cláusula sexta del aludido acuerdo.

A la par, el tribunal ponderó que el GCABA no rebatió que el SRFP no se encontraba inscripto en el Registro de datos relativo al Sistema de Videovigilancia²⁶ y meritó que la parte demandada no neutralizó la conclusión de la jueza de grado referida a que el sistema debía *“ser comprendido de modo integral, en su totalidad y no en forma compartimentada”*.

Allende lo dicho, el tribunal puso de relieve que el GCABA ninguna mención hizo con relación a la Guía para la Evaluación de Impacto en la Protección de Datos (EIPD)²⁷ como mecanismo de carácter preventivo tendiente a minimizar potenciales daños a la privacidad y cuya utilización es considerada beneficiosa para abordar los efectos que el uso del SRFP pudiera tener sobre los derechos de quienes transitan en la CABA. Tampoco repelió la trascendencia de la participación ciudadana en la materia²⁸.

En otro orden de ideas, el tribunal puso el énfasis en que el SRFP funciona a partir de la reunión del dato biométrico provisto por el RENAPER y la orden judicial incorporada a la CONARC, dando lugar al registro de búsqueda sobre el que trabaja el SRFP. En esa línea argumental, recalcó que el debate se centraba en el funcionamiento adecuado del SRFP *in totum*, por lo que la acción se dirigió contra el GCABA, en su calidad de creador y

²⁵ En virtud de lo establecido en el art. 3° de la Resolución N° 398/MJySGC/2019.

²⁶ De acuerdo con los arts. 495 de la Ley N° 5688 y 23 de la Ley N° 1845.

²⁷ Enmarcado en el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal o Convenio N°108, aprobado por Ley nacional N° 27.483, sancionada el 06/12/2018 y publicada el 02/01/2019 en el BORA N° 34.025.

²⁸ Sustentada en el art. 34 de la CCABA y su reglamentación, esto es, los Foros de Seguridad Pública (FOSEP) previstos en los arts. 17 a 20 de la Ley N° 5688.

operador del sistema, y como responsable de su puesta en marcha sin falencias que generen restricciones indebidas sobre los derechos de la ciudadanía, ya que él es quien eligió esta herramienta y el modo en que operaría.

A la par, la Sala remarcó que de la prueba producida surgía de que cuando el SRFP comenzó a funcionar en abril de 2019, se produjeron múltiples casos de falsos positivos y que hasta octubre de 2019 continuaron advirtiéndose errores del sistema que provocaron falsos positivos y demoras indebidas. A su vez, en noviembre de 2019, se dictó la Disposición N° DI-2019-7-APNRNR#MJ, cuyo art. 1° suspendió del CONARC, “la publicación de aquellos imputados cuyos datos filiatorios aportados impid[ieran] su correcta individualización, ya fuer[a] por carencia de Documento Nacional de Identidad o discordancias manifiestas entre los datos aportados y los correspondientes al DNI informado”, incluyendo en dos Anexos²⁹ el listado de las personas respecto de quienes se decidió suspender la aludida base de datos. Esa suspensión mantendría vigencia hasta que los organismos jurisdiccionales que hubieran dispuesto las medidas rectificasen o ratificasen los datos referidos o solicitaran de modo expreso mantener la publicación en los términos originales.

Luego, el tribunal destacó que en marzo de 2020 con el inicio de la pandemia y el establecimiento del “Aislamiento social, preventivo y obligatorio”, se produjo la suspensión del SRFP dispuesta en julio de 2020 y retroactiva a abril de ese mismo año³⁰, decisión que fue dejada sin efecto por Resolución N° 278/SSGA/2020³¹. El 20/10/2020 el RNR procedió a suspender el servicio de modo general, a los fines de la depuración de la base de datos³², aprobándose en el año 2021 el “Protocolo de Actuación para el Sistema de Consulta Nacional de Rebeldías y Capturas”, tendiente a agilizar el proceso de altas y bajas de las comunicaciones judiciales a dicha base de datos, mediante entre otros aspectos, la compulsa diaria de la misma³³.

En abril de 2021, se estableció una Coordinación específica del Departamento CONARC, con la finalidad de dotar al mismo de un mayor contralor y una mayor autonomía³⁴ y se asentó que como resultado de las medidas adoptadas se había logrado “depurar la indicada base de datos, de 46.000 a 33.000 registros, manteniéndose un permanente vínculo con los distintos operadores del sistema judicial con la finalidad de mantener actualizado dicho proceso de depuración”.

²⁹ El anexo I con aproximadamente dos mil cuatrocientos –2400– registros y el anexo II con más de seis mil cuatrocientos –6400–.

³⁰ Resolución N° 141/SSGA/2020, emitida el 13/07/2020 y publicada el 15/07/2020 en el BOCABA N° 5910.

³¹ Emitida el 04/12/2020 y publicada el 14/12/2020 en el BOCABA N° 6016.

³² Cfr. Nota N° NO-2020-70688753-APN-RNR# MJ, aludida en el Informe N° IF-2021-105080845-APN-RNR#MJ.

³³ Disposición N° DI-2021-1-APN-RNR#MJ.

³⁴ Cfr. lo expuesto por el RNR en el informe N° IF-2021-105080845-APN-RNR#MJ del 01/11/2021.

A juicio del tribunal, este detalle permite observar que el GCABA no pudo acreditar la inexistencia de errores del SRFP. Así, dados los avatares acaecidos desde la fecha en que se produjeron los falsos positivos (v. gr. suspensión parcial o total de la base de datos que nutre el SRFP o suspensión de este último mecanismo con motivo de la pandemia) y aun cuando ellos eventualmente no hubieran sido provocados por errores imputables directamente al manejo de la herramienta por parte del GCABA, este no logró demostrar la inexistencia de detenciones o demoras injustificadas de quienes transitan por la CABA con motivo de la utilización del SRFP. Esa imposibilidad de justificar la inexistencia de falsos positivos, provocada por la suspensión del SRFP, no habilita a concluir que el SRFP –actualmente– no arroje errores en la identificación de las personas buscadas.

Aunado a lo dicho, la Sala resaltó que el ejercicio irregular de las competencias por parte de las autoridades, con sustento en errores u omisiones en el cumplimiento de las competencias dadas por el ordenamiento jurídico, trasunta en una afectación directa y concreta a los derechos constitucionales a la libertad ambulatoria, a la autonomía personal, a la dignidad, a la igualdad de trato, y a todos los derechos que incidentalmente se ven restringidos a partir de la vulneración de aquellos (derecho a la intimidad personal, de reunión, a trabajar, etc.).

En otro orden de ideas, el tribunal estimó –según la información dada por la Dirección General de Asuntos Jurídicos de la Legislatura local el 01/11/2021– que la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia prevista en el art. 490 bis de la Ley N° 5688 no había sido constituida. No obstante, la Sala meritó –a raíz de informaciones periódicas³⁵– que dicha Comisión se habría constituido el 29/04/2022, aunque no se podía verificar si había ejecutado sus competencias de control.

Por otra parte, puso de relieve que la Resolución N° 398/MJySGC/2019 invitó a la Defensoría del Pueblo local a auditar el funcionamiento del SRFP, a cuyo fin se instruyó a la Secretaría de Justicia y Seguridad a gestionar la suscripción del pertinente convenio entre aquel Organismo y el MJyS, en el plazo de treinta (30) días. La Sala aclaró que dicha Resolución fue dictada con anterioridad a la sanción de la Ley N° 6339 y que la norma posterior –de mayor rango– no reguló con idénticos alcances que su predecesora la participación del órgano constitucional. Pese a ello, el Convenio suscripto entre el GCABA y dicho organismo que, al no haber sido denunciado por el demandado, mantiene su vigencia; así como las responsabilidades que la Ley N° 1845 puso a cargo de la Defensoría del Pueblo local en materia de protección de datos personales. De allí, el tribunal entendió la razonabilidad de sostener en cabeza de dicho organismo constitucional la intervención fiscalizadora del mecanismo que dio motivo al proceso.

³⁵ Ver: <https://www.telam.com.ar/notas/202204/591041-comision-legislativa-seguimiento-sistema-vigilancia-biometrica-caba.html> [Consulta efectuada por el tribunal].

En consecuencia, dijo que si –por un lado– los organismos llamados a ejercer el control del SRFP no pudieron llevar a cabo las funciones de auditoría que el plexo normativo les reconoció; y, por el otro, aquella herramienta estuvo sin operar debido al contexto pandémico y a la existencia de errores en la base de la CONARC, se desconoce sobre qué bases fácticas el GCABA asevera que el SRFP funciona correctamente.

4. PUNTOS CIEGOS SOBRE LOS CUALES CABE HACER FOCO

La principal tensión que se observa en el caso bajo estudio se manifiesta entre el dispositivo que el GCABA utiliza para satisfacer el deber irrenunciable de proveer el servicio esencial de seguridad y los derechos que la parte actora identifica como vulnerados con motivo de la utilización del SRFP.

Sin perjuicio de lo dicho, como cuestiones colaterales a esa tensión es posible advertir dos puntos ciegos sobre los cuales la sentencia de análisis no se explaya, esto es: el procedimiento de contratación del software en cuestión y el alcance de los secretos profesionales derivados de la propiedad intelectual. Creemos que vale la pena realizar ciertas reflexiones en torno a ellos por el impacto que tienen sobre el interés público.

4.1. Procedimiento de contratación del software en cuestión: contratación directa

La Ley N° 2095³⁶ de Compras y Contrataciones de la CABA establece diversas clases de procedimientos para canalizar las contrataciones públicas. Su art. 27 dispone que los procedimientos tipificados son: a) la licitación o el concurso; b) la contratación directa, y c) el remate o subasta inversa. Cada uno de ellos se rige por un régimen especial de acuerdo con las particularidades que los caracterizan.

Más allá de la variedad de procedimientos que la ley contempla, por regla general, la selección del contratista se realiza a través de los procedimientos de licitación o concurso públicos. Tanto la elección del procedimiento de selección, como de las modalidades del llamado a licitación o concurso, estará determinada por las características de los bienes o servicios a contratar, el monto estimado del contrato, y/o las condiciones de comercialización y configuración del mercado. Asimismo, la ley prevé que cualquiera de los procedimientos podrá llevarse a cabo a través de distintas modalidades o con combinación de ellas. En todos los casos deben cumplirse, bajo pena de nulidad, los principios³⁷ establecidos por el art. 7° de la Ley N° 2095.

³⁶ Sancionada el 21/09/2006 y publicada el 02/11/2006. Texto consolidado según Ley N° 6588, sancionada el 12/12/2022 y publicada el 10/11/2022 en el BOCABA N° 6517.

³⁷ Art. 7° Ley N° 2095: *“Principios generales que rigen las contrataciones y adquisiciones - Los principios generales a los que debe ajustarse la gestión de las contrataciones, teniendo en cuenta las particularidades de cada una de ellas son: 1. Principio de Libre Competencia [...]; 2. Principio de Concurrencia e Igualdad [...]; 3. Principio de Legalidad [...]; 4. Principio de Publicidad y Difusión [...]; 5. Principio de Eficiencia y Eficacia [...]; 6. Principio de Economía [...]; 7. Principio de Razonabilidad [...]; 8. Principio de Transparencia [...]; 9.*

Ahora bien, en lo que a nuestro análisis interesa, vale señalar que la empresa encargada de realizar el desarrollo del software del SRFP –DANAIDE S.A.– fue contratada a través de contratación directa, en los términos de lo dispuesto en el entonces vigente art. 28 inc. 6 de la Ley N° 2095³⁸.

Según consta en la web³⁹ del GCABA, el Pliego Único de Bases y Condiciones Generales fue publicado el 03/04/2019 a las 19.00 horas. Llamativamente, a las 19:02 horas –con una celeridad encomiable, ajena al usual proceder de la Administración– mediante Resolución N° 59/SSGA/19⁴⁰ se aprobó el Pliego de Bases y Condiciones Particulares y de Especificaciones Técnicas para la contratación de un servicio de análisis integral de video. En la motivación del acto se destacó que la contratación directa debe encontrarse debidamente fundada y ponderada por la autoridad competente, y que procede “sólo en los siguientes casos: [...] 6) cuando se trate de la reposición o complementación de bienes o servicios accesorios que deban necesariamente ser compatibles con los modelos, sistemas o infraestructura previamente adquiridos o contratados”. Además, el GCABA sostuvo que el objeto de dicha contratación “se funda[ba] en la necesidad de complementar el servicio de monitoreo por video y control de acceso vehicular (“Anillo digital”), oportunamente contratado en el marco de la Licitación Pública de Etapa Única N° 2900-0703-LPU16, incorporando nuevas tecnologías al mismo que permitan detectar a sujetos con pedido de captura, que ingresan a la Ciudad, a través de un sistema de reconocimiento facial”.

A la par, mediante dicha Resolución se llamó a contratación directa N° 2900-0472-CDI19 para el día 09/04/2019 por un monto estimado de dólares estadounidenses un millón quinientos noventa y ocho mil (USD 1.598.000) y se dispuso a efectuar la invitación de rigor a la firma DANAIDE S.A.

Luego, mediante la Resolución N° 98/SSGA/19⁴¹ se aprobó la contratación directa, bajo el entonces el art. 28 inc. 6 de la Ley N° 2.095, y el Decreto N° 326/GCABA/17 modificado por el Decreto N° 287/GCABA/18, y se adjudicó la contratación de un servicio de análisis

Principio de sustentabilidad [...]; 10. Principio de la vía electrónica [...]. Desde el inicio de las actuaciones hasta la finalización de la ejecución del contrato, toda cuestión vinculada con la contratación deberá interpretarse sobre la base de una rigurosa observancia de los principios que anteceden. Los principios señalados servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de la presente ley, como parámetros para la actuación de los funcionarios y dependencias responsables, y para suplir los vacíos en la presente ley y demás normas reglamentarias”.

³⁸ Actualmente, art. 29 inc. 6 de la Ley N° 2095 (texto consolidado según Ley N° 6588).

³⁹ Información disponible en:

<https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyvzUss83%7C5qmQHdIWCoEzPIKUOJAyRZ7kltC74K%7C7Tw11ctBR9dfFZZemaLoi969Lwy2BFPNowVGFQ7XOHCTEKW51rAObRlXsdfYAs0SFw==> [Consulta: 15/11/2023]

⁴⁰ Emitida el 03/04/2019 y publicada el 08/04/2019 en el BOCABA N° 5593.

⁴¹ Emitida el 22/04/2019 y publicada el 25/04/2019 en el BOCABA N° 5604.

integral de video a dicha firma por un monto total de dólares estadounidenses un millón quinientos once mil trescientos (USD 1.511.300).

Ahora bien, de la motivación de la Resolución N° 59/SSGA/19 –basada sobre el entonces vigente art. 28 inc. 6 de la Ley N° 2095–, se sigue que el GCABA perseguía la complementación del servicio de monitoreo por video y control de acceso vehicular (“Anillo digital”), oportunamente contratado en el marco de la Licitación Pública de Etapa Única N° 2900-0703-LPU16⁴². Vale decir que en el marco de dicha licitación la única oferta presentada fue la de DANAIDE S.A., la que resultó adjudicada mediante Resolución N° 667/MJYSGC/16⁴³.

De este modo, se vuelve plausible que, si en el marco de aquella licitación pública se presentó un solo oferente, se contrate de manera directa al mismo proveedor para la complementación de ese servicio.

Sin embargo, cabe memorar que en toda contratación deben primar la licitación pública como regla y los principios a los que alude el art. 7 de la Ley N° 2095. Aquí, el GCABA encorsetó legalmente su decisión en lo previsto en el entonces art. 28 inc. 6 de la Ley N° 2095 y en el principio celeridad, pero soslayó que eligiendo el procedimiento de contratación directa dejaba de lado los principios de libre competencia, de concurrencia e igualdad, de transparencia y, quizás, hasta el principio de sustentabilidad.

De esta manera, cabe concluir que, a menos que el GCABA contase con extraños poderes de oráculo, no es posible conjeturar que ante un llamado licitatorio para complementar los servicios del “Anillo Digital” no se hubieran presentado otros oferentes, por lo que estimo que, para mayor transparencia, dicha contratación debería haberse llevado a cabo por licitación pública. Máxime teniendo en cuenta el interés público comprometido: ya sea por los derechos fundamentales de la ciudadanía que, como señala Vaninetti (2023), con la implementación del SRFP podrían verse vulnerados, y por dejarse al erario sin opciones para obtener una mejor oferta.

4.2. Secreto profesional derivado de la propiedad intelectual

La Sala menciona en punto VII. d. (xi) de su sentencia, relativo al análisis de los agravios comunes, que *“es dable observar (v. prueba testimonial) que cierta información respecto del funcionamiento técnico del sistema no fue develada en esta causa”*.

⁴² Para mayor información ver:

<https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhz0jkKH6Y8uZIX3nFi8tXKyfwX7ektpuJ8uXjHqInsbmge0YwGERRROVoOyOkbmcnMwYZiJ0J3gm1EH23GkaoSuyEMTr9qVwgvmeE60vWZbxJA==> [Consulta 15/11/2023].

⁴³ Emitida el 27/09/2016 y publicada el 30/09/2016 en el BOCABA N° 4977.

En el marco de la audiencia testimonial⁴⁴, el desarrollador de software de DANAIDE S.A. sostuvo no poder revelar información relacionada con el “motor de búsqueda” –no creado por él–, puesto que se trataba de información confidencial y que él tenía un contrato con dicha empresa que le impedía divulgar ese tipo de información.

4.2.1. Regulación normativa

En la República Argentina la protección de los secretos comerciales y la información confidencial está dada principalmente por lo dispuesto en el art. 39.2 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (“ADPIC”)⁴⁵, en la Ley N° 24.766⁴⁶ de Confidencialidad y en el art. 156 del Código Penal – en adelante, CP–.

El art. 39.2 del ADPIC establece: *“2. Las personas físicas y jurídicas tendrán la posibilidad de impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos⁴⁷, en la medida en que dicha información: a) sea secreta en el sentido de que no sea, como cuerpo o en la configuración y reunión precisas de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y b) tenga un valor comercial por ser secreta; y c) haya sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla”*.

Por su parte, casi con idénticas palabras, el art. 1º de la Ley de Confidencialidad N° 24.766 también protege la información confidencial de su divulgación no autorizada.

⁴⁴ Audiencia celebrada el 06/06/2022. Testimonio del señor Emiliano Carlos Schmith. Ante la pregunta del juez de grado, por la que le requirió que describa todo el funcionamiento de DANAIDE S.A. en torno al SRFP en el ámbito de la CABA, el testigo dijo: *“Es el que provee el software en su totalidad. [...] Desarrolla el software, lo instala, lo deja en funcionamiento para que la Ciudad lo pueda usar, y le da soporte. [...] El software tiene muchas partes. DANAIDE desarrolla prácticamente todo el software, excepto una parte muy específica: el motor de reconocimiento”*. Frente a ello, el juez preguntó cuál es el origen de ese motor de reconocimiento, y el testigo manifestó: *“No sé si puedo contestar esa pregunta. Yo tengo un contrato de confidencialidad con la empresa”*. El juez replicó: *“Está en una audiencia judicial y tiene la obligación de contestar”* y el testigo dijo: *“El que debería contestar eso, por ahí, es el presidente de la empresa que es el que hace los contratos. Yo soy ajeno a eso”*. Luego el juez preguntó: *¿Usted desconoce?*, a lo que el testigo respondió: *“No conozco la forma contractual y firmé un contrato donde no puedo divulgar ese tipo de información”*.

⁴⁵ Ratificado por Ley N° 24.425, sancionada el 07/12/1994 y publicada el 05/01/1995 en el BORA N° 28.054.

⁴⁶ Sancionada el 18/12/1996 y publicada el 30/12/1996 en el BORA N° 28.553.

⁴⁷ El texto del Acuerdo dispone que *“[a] los efectos de la presente disposición, la expresión ‘de manera contraria a los usos comerciales honestos’ significará por lo menos las prácticas tales como [...] la adquisición de información no divulgada por terceros que supieran, o que no supieran por negligencia grave, que la adquisición implicaba tales prácticas”*.

Finalmente, el art. 156⁴⁸ del CP reza que: *“Será reprimido con multa de pesos mil quinientos a pesos noventa mil e inhabilitación especial, en su caso, por seis meses a tres años, el que, teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa”*.

4.2.2. Protección del software

Conforme lo define la Real Academia Española⁴⁹, el software consiste en un conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Al respecto, señala Mille (1988) que los programas de computación, como el resto de los productos resultantes del proceso de creación del software, son considerados como “obras” en virtud de ser un producto del ingenio humano, en la medida que: a) constituyen expresiones concretas y formalizadas de ideas; b) expresan procedimientos, pero no equivalen a éstos, en cuanto no se dirigen a alterar la realidad sino a indicar un camino lógico a la mente humana; c) constituyen el resultado de un acto intelectual creativo; d) cuando son obras originales o derivados de una original con la autorización de su autor, resultan por definición de la labor personal de su creador; e) existe una crecida cuota de esfuerzo intelectual. No se trata de una mera labor manual o técnica o de la ejecución de la creación intelectual de un tercero; f) adquieren expresión concreta, que se sustenta sobre una base material permanente.

A su vez, tal como apunta Flores (2014) “los mecanismos para hacer operativa la protección del software han de ser múltiples. Entre ellos [...] patentes; diseños y modelos; marcas; derechos de autor; secreto industrial y profesional; competencia desleal; normas penales; institutos del derecho privado (responsabilidad civil, enriquecimiento sin causa, autonomía de la voluntad”.

4.2.3. ¿Es posible la dispensa judicial del deber de confidencialidad en una audiencia testimonial donde se halla comprometido el interés público?

El hecho de que el testigo haya asegurado tener un contrato de confidencialidad con DANAIDE S.A. –que, por cierto, no presentó en la audiencia– nos conduce a analizar cuáles son los alcances del secreto profesional invocado para evadir dar respuesta al tribunal en torno al “motor de búsqueda”.

En relación con ello, Gabet (2022) expresa que tanto el obrar de buena fe como el deber de fidelidad del trabajador son dos pilares fundamentales que no necesitan de una norma

⁴⁸ Sancionado el 30/09/1921 y publicado el 03/11/1921 en el BORA N° 8300. Multa actualizada por el art. 1° de la Ley N° 24.286 (BORA del 29/12/1993).

⁴⁹ Real Academia Española: Diccionario de la lengua española, 23.ª ed., [versión 23.6 en línea]. <<https://dle.rae.es>> [Consulta: 13/11/2023].

interna de la empresa para que resulte obligatorio su acatamiento, ya que las políticas de empresa son complementarias al marco normativo que establece la legislación laboral.

Por otro lado, siguiendo a Giay y Fernández (2013) no caben dudas de que los secretos comerciales o industriales son hoy en día una de las herramientas de mayor importancia para las empresas a fin de destacarse y tomar ventajas en un mercado cada vez más competitivo. En especial, en las industrias relacionadas con la tecnología de la información (denominadas industrias "IT"), dada la vertiginosa evolución de estas tecnologías, lo que en breve tiempo las torna obsoletas.

Considerando lo antedicho, si bien el art. 352 del Código Contencioso Administrativo y Tributario de CABA⁵⁰ –en adelante, CCAyT– es claro al establecer que “El/la testigo puede rehusarse a contestar las preguntas: 1. Si la respuesta lo expusiere a enjuiciamiento penal o comprometiera su honor. 2. Si no pudiere responder sin revelar un secreto profesional, militar, científico, artístico o industrial”, cabe preguntarnos: ¿el deber de confidencialidad no puede ser dispensado judicialmente en el marco de una audiencia testimonial donde está comprometido el interés público?

Pensemos que el inc. 1 del citado art. 352 del CCAyT alude a la posibilidad de enjuiciamiento penal. Pues bien, el citado art. 156 del CP, refiere a aplicar sanción al “que, teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa”. Aquí aparece el primer alumbramiento, dado que la revelación del secreto tendría una justa causa: el requerimiento judicial en el marco de un proceso que imbrica el interés público.

A la par, dado que el art. 39.2 del ADPIC ya transcripto establece: “Las personas físicas y jurídicas tendrán la posibilidad de impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos...”, cabe formular un nuevo interrogante: ¿podría sostenerse que la magistratura en un Estado Constitucional de Derecho podría usar la información brindada por un testigo para un “uso comercial deshonesto”? La respuesta aparece prístina: claro que no, la judicatura debe velar por la plena vigencia de los derechos fundamentales y jamás podría utilizar información con fines ilícitos o deshonestos.

A su vez, la citada Ley N° 24.766, dispone en su art. 3° que: “Toda persona que, con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a una información [...] y sobre cuya confidencialidad se los haya prevenido, deberá abstenerse de usarla y de revelarla sin causa justificada o sin consentimiento de la persona que guarda dicha información o de su usuario autorizado”. Sin embargo, lo

⁵⁰ Ley N° 189, sancionada el 13/05/1999 y publicada el 28/06/1999 en el BOCABA N° 722. Texto consolidado según Ley N° 6588.

interesante de esta ley es que añade en su art. 10 que: “Quedaría exceptuado de la protección del artículo 4^o⁵¹, la información cuya publicación sea necesaria para proteger al público o cuando se adopten medidas para garantizar la protección de dicha información contra todo uso comercial deshonesto”.

De la lectura sistemática de los fragmentos transcritos, fácil es colegir que el órgano legisferante ha querido proteger los secretos de la propiedad intelectual contra todo uso comercial deshonesto, mas no contra el daño que pudiera causarse al interés público. En efecto, el referido art. 10 pone de relieve que cede la protección del secreto cuando la publicación de la información sea necesaria, justamente, para proteger al público.

Sánchez Herrero (2007), en un trabajo en el que intenta explicar cómo operan distintas causas sobre las motivaciones y limitaciones criminales –en nuestro caso, la violación de secretos en el marco de la propiedad intelectual– entiende que la persona es libre y que, si bien puede verse condicionada por las circunstancias, no está predeterminada a actuar en un determinado sentido.

Pues bien, ¿cuál hubiera sido, a nuestro humilde criterio, el *as* de la magistratura para obtener dicha información?: informar al testigo que las respuestas en torno al “motor de búsqueda” serían tomadas únicamente en presencia del juez y el actuario, y que el testimonio en torno a ese punto sería reservado en la caja fuerte del juzgado, sin posibilidad de ser visto por las partes, ni por cualquier persona con acceso al expediente, salvo la magistratura, dado que el interés público estaba comprometido y, por tanto tenía obligación de responder. De ese modo, se hubiera dotado de garantías al testigo velando por el interés público, sin violar la ley. Como dice Rosler (2020), “*la ley es la ley*”.

Vale añadir que, si en caso de que el testigo hubiera declarado en torno al “motor de búsqueda” y luego la empresa hubiera formulado una denuncia en su contra o hubiera resuelto su despido, aquél habría contado con los medios legales para repeler dicho temperamento, amparándose en el requerimiento judicial.

5. COLOFÓN

A lo largo de estas líneas hemos visto el derrotero que siguió el amparo iniciado hasta culminar en la sentencia de la Sala I de la Cám.CATyRC que rehabilitó el funcionamiento del SRFP. Dicha rehabilitación quedó supeditada a la constitución y debido funcionamiento de los órganos de control, a la realización de las investigaciones y

⁵¹ Art. 4° de la Ley N° 24.766: “Para los casos en que se solicite la aprobación del registro o autorización de comercialización de productos que utilicen nuevas entidades químicas que no tengan registro previo ni en la Argentina ni en cualquier otro país, deberá presentarse a la autoridad sanitaria local información que acredite la eficacia e inocuidad del producto. En la medida que esta información reúna los requisitos del artículo 1° y sea resultado de un esfuerzo técnico y económico significativo, será protegida contra todo uso comercial deshonesto tal como se define en la presente ley y no podrá ser divulgada”.

pruebas necesarias sobre el software que utiliza para determinar si tiene un impacto diferenciado según las características personales de los individuos afectados, y a dar publicidad de la existencia de esta herramienta, su funcionamiento y las reglas jurídicas que lo rigen, en el ámbito de los FOSEP y a los vecinos y organizaciones que así lo soliciten, para puedan formular observaciones.

Más allá de eso, al no haberse obtenido declaración testimonial en torno al origen y funcionamiento del “motor de búsqueda”, por más que esta sentencia supedita la rehabilitación del SRFP a los controles de los órganos pertinentes, lo cierto es que estos se encontrarán con el mismo valladar del juez de primera instancia al intentar recabar la información, con la peculiaridad que ellos, a diferencia de aquél, no gozan de *imperium* para obtenerla.

Hemos visto que la sentencia en cuestión no se explaya ni sobre el procedimiento de contratación elegido por el GCABA ni sobre el medio de prueba testimonial desperdiciado que podría haber arrojado mayor luz sobre el total funcionamiento del SRFP, al que quienes transitamos la CABA una vez que esté operativo nos veremos expuestos. Estas dos cuestiones tienen vinculación, por un lado, con el destino de los recursos del erario y, por el otro, con el destino de datos sensibles de la ciudadanía. Todo ello hace, en definitiva, ni más ni menos que al interés público.

Finalmente, y sin ánimos de caer en una suerte de paranoia, si el GCABA dice velar por la seguridad de la ciudadanía: ¿pueden él o la magistratura garantizarnos que no estemos siendo vigilados desde otros Estados u organizaciones internacionales? Creemos que no, ya que ninguno de ellos cuenta con información sobre el “motor de reconocimiento” que provee una misteriosa empresa extranjera. El Gran Hermano existe, pero es deber de la Administración y la judicatura ayudarlo a ser su mejor versión, dentro del marco de las competencias que les tocan.

BIBLIOGRAFÍA

Flores, Álvaro B. 2014. “La promoción de la industria del software en Argentina”, cita online: TR LALEY AR/DOC/4962/2014.

Gabet, Emiliano A. 2022. “Revelación de información confidencial como causa del distracto”, cita online: TR LALEY AR/DOC/1958/2022.

Giay, Gustavo; Fernández, Diego. 2013. “Protección de los secretos comerciales. Doctrina de la revelación inevitable”, cita online: TR LALEY AR/DOC/2990/2013.

Mille, Antonio. 1988. “Evolución de las ideas jurídicas sobre el software (en la doctrina y el derecho comparados)”, LA LEY 1988-D 1210.

Real Academia Española: Diccionario de la lengua española, 23.ª ed., [versión 23.6 en línea]. <<https://dle.rae.es>> [13/11/2023].

Rosler, Andrés. 2020. *La ley es la ley*, 1ª ed., Katz, Ciudad Autónoma de Buenos Aires.

Sánchez Herrero, Andrés. 2007. “Sobre la observancia de los derechos intelectuales”, cita online: TR LALEY AR/DOC/3266/2007.

Vaninetti, Hugo A. 2023. “Implementación del Sistema de Reconocimiento Facial de Prófugos (SRFP) de la Ciudad Autónoma de Buenos Aires. El necesario resguardo de los derechos y garantías constitucionales”, cita online: TR LALEY AR/DOC/1470/2023.