

# EL SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS DEL GCABA y su lesión a los derechos a la privacidad y autodeterminación informativa

NATALIA PACHECO

Revista de la Escuela del Cuerpo de Abogados y Abogadas del Estado |  
Octubre 2023 | Año 7 N° 10 | Buenos Aires, Argentina (ISSN 2796-8642) |  
pp. 175-190

*A propósito de la sentencia de 1° Instancia del Caso “Observatorio de Derecho Informático Argentino (ODIA) y otros c/ GCABA s/ amparo” de fecha 7 de septiembre de 2022<sup>1</sup>.*

**Resumen:** En la investigación se tomó conocimiento del caso judicial y se procedió al cotejo de la normativa implicada, por un lado se analizó el Sistema de Reconocimiento Facial de Prófundos puesto en funcionamiento en virtud de la Resolución 398/MJYSGC/19, según lo establecido por un Convenio anterior cruzaba datos personales biométricos entre bases de datos de la CONARC (Registro Nacional de Reincidencia) y del Registro Nacional de las Personas permitía “matchear” imágenes faciales de personas que transitaban las calles de CABA en puntos determinados e ingresaban en Estaciones de Tren o subtes y podían dar alertas de personas buscadas por la Justicia, pero en muchos casos dieron falsos positivos ordenando la detención/demora de personas que no correspondían a ningún requerido judicial. Se valoraron las pericias técnicas e informes produci-

1 SENTENCIA, 7 de Septiembre de 2022, JUZGADO EN LO CONTENCIOSO ADMINISTRATIVO Y TRIBUTARIO NRO 4. CIUDAD DE BUENOS AIRES, CIUDAD AUTÓNOMA DE BUENOS AIRES, Magistrados: Elena Amanda Liberatori disponible online [http://www.sajj.gov.ar/FA22370014?utm\\_source=newsletter-semanal&utm\\_medium=email&utm\\_term=semanal&utm\\_campaign=jurisprudencia-provincial](http://www.sajj.gov.ar/FA22370014?utm_source=newsletter-semanal&utm_medium=email&utm_term=semanal&utm_campaign=jurisprudencia-provincial) al 1/11/2022



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 2.5 Argentina

dos y quedo probado que al momento de implementarse el Sistema no se había realizado un estudio de evaluación de impacto en datos personales, las bases no se encontraban inscriptas en el Registro correspondiente, lo que las convertía en bases ilícitas y tampoco había intervenido el órgano de control de datos personales de CABA, la Defensoría del Pueblo mediante el Centro de Protección de Datos ni se había auditado el funcionamiento del sistema, lesionando así derechos constitucionales como el de la privacidad autodeterminación informativa, protección de datos personales y principios y garantías constitucionales básicas del Estado Constitucional de Derecho.

**Palabras clave:** reconocimiento facial- datos personales- inteligencia artificial- privacidad

**Antecedentes:** La Ciudad Autónoma de Buenos Aires fue el escenario propicio en los últimos años para el uso y abuso de las IA disponibles y aptas para ejercer facultades coactivas del Estado y mejorar la seguridad, a la vez, pueden llegar a lesionar arbitrariamente los derechos a la autodeterminación informativa, a la privacidad, intimidad y de protección de datos personales así como violar principios y garantías como la presunción de inocencia y el debido proceso sustantivo que son la base fundamental del Estado Constitucional de Derecho.

Ante el crecimiento del delito en el ámbito de la CABA, el aumento de la pobreza y el desempleo sumado a la necesidad de demostrar eficiencia en la gestión pública las autoridades implementan sistemas de IA bajo condiciones a cumplir que se encuentran previstas en la normativa vigente pero que no se cumplen, verifican ni auditan debidamente.

En este marco surgió el caso del Sistema de Reconocimiento Facial de Prófugos implementado en el ámbito de la Ciudad Autónoma de Buenos Aires, por la Resolución 398/MJYSGC/19<sup>2</sup> que en líneas generales claramente prevé:

*“...la utilización del sistema integral de video vigilancia está regida por el principio de proporcionalidad y razonabilidad...  
...sólo podrá emplearse cuando resulte adecuado, en una situación concreta, para asegurar la convivencia ciudadana,*

---

2 Resolución 398/MJYSGC/19 disponible online [https://documentosboletinoficial.buenosaires.gob.ar/publico/ck\\_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf](https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf) al 1/11/2022

*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...  
...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 conformidad con los principios consagrados en la Constitución Nacional y la Constitución de la Ciudad Autónoma de Buenos Aires...  
...la Ley Nacional N° 25.326 de Protección de los Datos Personales establece que no será necesario el consentimiento del titular de los datos para el tratamiento de los mismos cuando: a) los datos se obtengan de fuentes de acceso público irrestricto; y b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;...”*

Dicho sistema se alimenta de otras bases de datos, en las condiciones que la misma resolución explica:

*“... por el Decreto PEN N° 346/09<sup>3</sup> se creó la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC), del Registro Nacional de Reincidencia del Ministerio de Justicia y Derechos Humanos de la Nación, el cual se conforma con las comunicaciones que las autoridades judiciales realizan de toda medida restrictiva a la libertad ambulatoria que se dicta en el marco de una causa penal, en cualquier jurisdicción del país (ámbito federal, nacional, provincial y de la Ciudad Autónoma de Buenos Aires)...  
...el Decreto PEN N° 1766/11<sup>4</sup> (modificado por Decreto PEN N° 243/17) creó el “Sistema Federal de Identificación Biométrica para la Seguridad” (SIBIOS), a fin de contribuir a la identificación de personas mediante información brindada a sistemas automatizados de identificación de huellas digitales y rostros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad...  
... se celebró un Convenio de Cooperación Técnica entre el Registro Nacional de las Personas (RENAPER) y este Ministerio de Justicia y Seguridad, mediante el cual dicho Organismo facilitará,*

3 Decreto PEN N° 346/09 disponible online en <http://servicios.infoleg.gob.ar/infolegInternet/anexos/150000-154999/152565/norma.htm> al 1/11/2022

4 Decreto PEN N° 1766/11 disponible online en <http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm> al 1/11/2022

*por la vía de excepción prevista en el artículo 23, inciso 2) de la Ley Nacional N° 25.326<sup>5</sup>, el acceso a la información disponible en sus sistemas informáticos tendiente a identificar y/o verificar la identidad de las personas prófugas, conforme a requerimientos efectuados por el Ministerio Público Fiscal, y los Poderes Judiciales Nacional, Provincial y de la Ciudad Autónoma de Buenos Aires...  
 ...RENAPER facilitará los registros biométricos que el Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires solicite de acuerdo a los requerimientos fiscales y judiciales correspondientes, dejando expresamente aclarado que no se trata de la totalidad de las fotografías de la población sino solamente las de aquellas personas requeridas por la magistratura...  
 ...Invitar a la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires a auditar el funcionamiento del Sistema de Reconocimiento Facial de Prófuagos”.*

También se determinaron en la norma las condiciones para su operatoria:

*“...será empleado únicamente para tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial de la Nación, Provincial y de la Ciudad Autónoma de Buenos Aires, como así también para detección de personas buscadas exclusivamente por orden judicial, registradas en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC). Salvo orden judicial, se encuentra prohibido incorporar imágenes y registros de otras personas que no se encuentren registradas en el CONARC...  
 ... se integra con la totalidad de los registros incorporados en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC) y con los datos biométricos consultados del Registro Nacional de las Personas (RENAPER), debiendo corresponder estos últimos única y exclusivamente a personas que registren orden judicial de restricción de la libertad registradas en la base del CONARC...  
 ... La Policía de la Ciudad no está autorizada a ceder tales archivos a ninguna otra autoridad administrativa de la Ciudad...  
 ... La operación del Sistema de Reconocimiento Facial de Prófuagos estará a cargo del Centro de Mo-*

---

5 Ley 25.326 de Protección de Datos Personales disponible online en <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm> al 1/11/2022

***nitoreo Urbano (CMU) de la Policía de la Ciudad. ...Toda vez que el sistema detecte una coincidencia, el Centro de Monitoreo Urbano procederá a generar una carta de servicio y dará aviso al personal policial correspondiente, actuando siempre de conformidad con los protocolos que rigen la Línea de Atención de Emergencias 911... ... cumplida la orden judicial de restricción de la libertad, o que la misma haya cesado, los datos personales tratados deberán ser destruidos”.***

Sin embargo, la realidad demostró que las consecuencias de su implementación no fueron del todo beneficiosas. Numerosas organizaciones no gubernamentales recibieron denuncias por situaciones irregulares de detenciones en puestos claves de la Ciudad, así el Observatorio de Derecho Informático Argentino (OIA), el Centro de Estudios Legales y Sociales (CELS) y varios *amicus curiae* como la ACIJ, la CORREPI y la Fundación Vía Libre entre otros decidieron presentar el amparo de la sentencia que comentaré.

Entre los fundamentos para iniciar la acción los de mayor relevancia son:

1.- El SRFP funciona mediante la comparación de las características biométricas de dos rostros; las IA deben aprender cuando se trata de la misma persona y cuando no. Lo que se logra a partir de una base de datos de distintas caras y mediante una “carga” de información constante, sin tener en cuenta la base de datos biométricos a la cual contrastar; esa base es la memoria para mejorar el funcionamiento de la Inteligencia artificial y no hace diferencias entre la base de datos de la CONARC sino que toma la totalidad de los rostros que pasen por la cámara.

2.- Se producen ciertas inconsistencias: falencias e irregularidades como la creación de “falsos positivos”: elige a personas con similares características dando datos erróneos de alertas, el SRFP tiene una efectividad que se encuentra por debajo del 50%.

3.- Su utilización implica un prejuizgamiento de los habitantes de CABA, una falta de respeto a los Derechos Humanos, al derecho a la privacidad, a la protección de los datos personales, generando una práctica discriminatoria contra las mujeres y minorías incumpliendo los Tratados internacionales de derechos humanos.

En este marco resultan lesionados derechos y principios constitu-

cionales que a continuación se detallan:

- Principio de presunción de inocencia: cualquier alerta que derive del uso de este sistema habilita la intervención policial para detener de manera intempestiva y pesa sobre esa persona una presunción de culpabilidad, se invierte el principio de inocencia y son los afectados quienes deben brindar explicaciones al Estado de porque no tienen nada que ver con la detención que se esta llevando a cabo.
- Derecho a la privacidad: en el procedimiento para determinar si los rostros que una camara de videovigilancia esta captando estan efectivamente en la base de datos del CONARC, la misma debe comparar todas las caras que surgen de las imágenes tomadas por la policia y realizarles un “tratamiento” para determinar si son o no de personas que se encuentran en esa base de datos. Es decir, se toman datos personales de carácter sensible como es la imagen, sin haber requerido y adquirido el consentimiento previo de cada uno de ellos.
- Principio de debido proceso sustantivo: se aprehende y detiene a una persona, sin las debidas garantías de procedimiento, defensa y juicio previo
- Principio de Razonabilidad: Manifiesta desproporcionalidad entre la medida implementada y los fines perseguidos. El Estado local busca garantizar “seguridad” a su comunidad pero introduciendo un elemento riesgoso que vulnera los derechos a la privacidad, intimidad, autodeterminación informativa y protección de datos personales de manera desproporcionada, con la utilización de un sistema que carece de los minimos elementos de cuidado y precaución.
- Entre las normas que se encuentran vulneradas se pueden mencionar:
- La normativa prevista por la CADH<sup>6</sup>, su art. 7 el derecho a la libertad persona y a la presunción de inocencia del art. 8, el art. 11 nadie puede ser objeto de injerencias arbitrarias o abusivas sobre su vida privada. También contenidos en la DUDH y el derecho a la igualdad, el en el Pacto Internacional de Dere-

---

6 Convención Americana sobre Derechos Humanos CADH disponible online en <http://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/28152/norma.htm> al 1/11/2022

chos Económicos Sociales y culturales, y en el Pacto de los Derechos Civiles y Políticos, la Convención Internacional sobre la Eliminación de todas las formas de discriminación Racial, la Convención sobre la eliminación de todas las formas de discriminación contra la mujer, todos estos instrumentos jerarquizados por el art. 75 inc. 22 de la CN. A su vez, el art. 16, el art. 18 y el art. 19 de la Constitución Nacional.

- La Constitución de la Ciudad Autónoma de Buenos Aires<sup>7</sup> garantiza en el art. 10 que los derechos y garantías no pueden ser negados ni limitados por la omisión o insuficiencia de su reglamentación, se reconoce y garantiza el derecho a ser diferente no admitiéndose discriminaciones por raza, etnia, género, edad, orientación sexual, religión, ideología, opinión caracteres físicos, condición psicofísica, social, económica o circunstancias de distinción, exclusión, restricción o menoscabo, también garantiza el derecho a la privacidad, intimidad, y confidencialidad como parte inviolable de la dignidad humana conforme art. 12 y la libertad como parte inviolable de la dignidad según el art. 13, también establece que el Gobierno de la Ciudad coadyuva a la seguridad ciudadana desarrollando estrategias y políticas multidisciplinarias de prevención del delito y la violencia diseñando y facilitando canales de participación comunitaria mediante el art. 34.
- La ley 27483<sup>8</sup> que aprobó el Convenio 108 y su protocolo adicional del Consejo de Europa cuyo objeto es el tratamiento automatizado de datos personales, es decir, sobre la información personal de toda persona física identificada o identificable y los Estados deben comprometerse a aplicar todas las medidas necesarias para que se protejan los datos contenidos en registros públicos o privados. Se hace alusión a una especial protección a aquellos datos que revelen origen racial, las opiniones públicas, convicciones religiosas, preferencias sexuales, datos de salud, que no podrán ser tratados automá-

---

7 Constitución de la Ciudad Autónoma de Buenos Aires disponible en [http://www.infoleg.gob.ar/?page\\_id=166](http://www.infoleg.gob.ar/?page_id=166) al 1/11/2022

8 Ley 27483 aprobatoria del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personales disponible online en <http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318245/norma.htm> al 1/11/2022

ticamente a menos que el derecho interno de las garantías apropiadas y deberán tomarse las medidas de seguridad correspondientes para la protección de los mismos para evitar la destrucción no autorizada, o la pérdida de los mismos, así como el acceso, la actualización o difusión no autorizada.

- En cuanto a la prueba presentada por la demandada, el MJS CABA informó al respecto que:
- En virtud del CONVENIO DE COOPERACIÓN TÉCNICA ENTRE RENAPER Y MJYS de CABA

***“...el RENAPER facilita por la vía de excepción art. 23 inc. 2) Ley 25326, el acceso a la información disponible en sus sistemas informáticos tendiente a identificar o verificar la identidad de personas humanas sobre las cuales el Ministerio desarrolle las tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial Nacional, Provincial y de la CABA...”***

***“RENAPER no remite a esta jurisdicción “datos biométricos” de ninguna persona: en todo caso, la fotografía asociada al DNI que transfiere al ente nacional será objeto de ese particular tratamiento técnico con la finalidad de identificar y aprehender personas requeridas por el Poder Judicial”.***

Sin embargo, dicha información deviene errónea ya que la fotografía como archivo de imagen asociada a una persona física deviene un dato biométrico, más aún referida a un DNI que a su vez tiene cargada la huella digital.

Existe a su vez otro informe probatorio en la causa, el de la Defensoría del Pueblo de CABA que hizo saber que:

- El GCABA no realizó la Evaluación de Impacto en la Privacidad (EIP)<sup>9</sup> que sí se realizó en otros países al ser implementado para determinar la justificación, proporcionalidad, legítimi-

---

9 Evaluación de Impacto en Protección de Datos Personales disponible online en [https://www.argentina.gob.ar/sites/default/files/guia\\_final.pdf\\_al\\_1/11/2022](https://www.argentina.gob.ar/sites/default/files/guia_final.pdf_al_1/11/2022) es un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales. Dicho tratamiento puede provocar impactos en los derechos de las personas que deben ser de algún modo identificados, gestionados, minimizados o eliminados para cumplir con la normativa vigente.

dad y necesidad de su uso a fin de determinar el impacto y la posible afectación a DP y otros DDHH (Guía de Evaluación en PDP de la AAIP)

- No se cumplió con la constitución e intervención de la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia integrada por Presidentes de Comisiones de Justicia y Seguridad y 3 diputados designados por las por la vicepresidencia primera sin perjuicio de que dicha Comisión convoque a especialistas de la Soc. Civil
- No se enviaron informes a la Defensoría del Pueblo CABA (órgano de control de PDP de CABA) sobre especificaciones técnicas del software, modificaciones técnicas de los dispositivos, criterio de instalación continuidad de los sistemas de videovigilancia.
- En esta misma línea observó además que todos los registros que se hicieran por el SRFP deberían, al contener datos personales, estar inscriptos en el Registro de Datos que funciona en el Centro de PDP para que dicha base sea lícita, requisito que sólo se cumple al estar inscripta (art. 4 inc. 2 Ley 1845<sup>10</sup>).

Por su parte, el MJDH en su informe indicó explicando las funciones de la CONARC que es el Sistema de Consultas Nacional de Rebeldías y Capturas que funciona dentro del Registro Nacional de Reincidencia y sirve para brindar información de un sistema punto a punto y de manera actualizada de la totalidad de los autos de rebeldía, capturas, averiguación de paradero y comparendos de su base de datos.

Explicó que en 2016 se dispuso que dicha base se publicara en el Portal de Datos Abiertos de la Justicia Argentina, pero a partir de 2021 se excluyó del citado portal ya que la publicidad de su contenido entraría en conflicto con la normativa específica de Protección de Datos Personales.

Por lo que concluye que es de consulta entre otros actores del sistema de seguridad pública, Fuerzas de Seguridad, policías provinciales y de la Policía de CABA y su utilización puede ocasionar inconvenientes y generar un “falso positivo” y aclaró que no se firmó

---

10 Ley 1845 de Protección de Datos Personales en CABA disponible online en <https://www.argentina.gob.ar/normativa/provincial/ley-1845-123456789-0abc-defg-548-1000xvorpvel/actualizacion> al 1/11/2022

ningún convenio con MJYS CABA ni con la Defensoría local, ni se lo convocó por la Comisión de la Legislatura. En cuanto a los falsos positivos detalló que son fallas en los datos patronímicos de las personas humanas incluidas por información falsa brindada por la propia persona humana, o por errores involuntarios de parte de los operadores de sistema judicial.

En otro orden de ideas, para enriquecer la etapa probatoria de la causa se realizó una inspección de constatación al Centro de Monitoreo Urbano (donde están localizados los servers), el lugar físico de la base operativa de la IA del SRFP y permitieron contrastar empíricamente ciertos detalles:

## **ARQUITECTURA TÉCNICA DE LA IA - LA AUTOMATIZACIÓN:**

La operatoria se realiza todas las mañanas cuando machea contra el CONARC y pregunta altas y bajas y automáticamente cuando llega un DNI nuevo, se le manda el DNI y te devuelve la foto. En ese momento se arma el registro para poder realizar el reconocimiento facial. Es un proceso automatizado. En la migración de datos de CONARC y del RENAPER no hay actividad humana, es un proceso de validación. Se da un DNI, hay un proceso armado, auditado, que valida el dato y esa validación es la que corresponde.

Las autoridades de la CABA indicaron que a la fecha de la inspección la parte física, estaba prendida, pero todo lo que es las máquinas virtuales, que son las que operativizan el software estaban apagadas.

El SRFP trabaja sobre 572 puntos del sistema facial, la mayoría del triángulo inferior del rostro, hay 300 cámaras con licencia para el uso de este sistema, depende de las eventualidades a cubrir se puede variar de lugar y se nutre del Sistema CONARC del Registro Nacional de Reincidencia. Mediante las cámaras de videovigilancia capta imágenes que se visualizan y procesan en el Centro de Monitoreo Urbano de la Policía de CABA y las coteja con los datos biométricos de CONARC y en caso de advertir una coincidencia, se emite una alerta para que el personal policial actúe.

Finalmente, a la hora de evaluar el material probatorio y la normativa aplicable se hizo referencia entre otros a:

La Guía para la evaluación de impacto en la protección de datos personales, que según mencionó la Defensoría del Pueblo de la

CABA, sirve para disminuir los riesgos que el uso de nuevas tecnologías, el tratamiento automatizado de datos y la IA que fueron elaborados por la AAIP Argentina y su órgano par de Uruguay cuya finalidad es minimizar los potenciales daños a la privacidad.

El tratamiento de datos personales puede causar impactos negativos en los derechos de las personas, que deben ser identificados, gestionados, minimizados y eliminados para cumplir con la normativa vigente, esta EIDP es un procedimiento que los responsables de bases de datos deben realizar para legitimar sus procedimientos para poner en funcionamiento nuevos proyectos o incorporar nuevos sistemas de IA que prevean tratamiento de información personal.

La ley 25326, de Protección de datos personales a nivel nacional resguarda y protege a nivel interno toda la información personal que se encuentre almacenada en archivos de responsables de datos públicos o privados, garantiza de esta manera el derecho al honor, a la intimidad, el acceso a la información y su control en cuanto a la pertinencia, finalidad, y razonabilidad para el tratamiento o el efectivo cumplimiento de la actualización, bloqueo o supresión cuando no corresponda su tratamiento. En su artículo 5 prevé que el tratamiento de datos personales será ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito u otro medio y sin embargo no será necesario cuando los datos se obtengan de fuentes de acceso irrestricto o se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

En lo que atañe a este caso en particular, es aplicable el inc. 2 art. 23 que establece que el tratamiento de datos personales con fines de defensa nacional o seguridad pública puede realizarse por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia sin consentimiento de los afectados y quedará limitado a los supuestos y categoría de datos necesarios para el ***estricto cumplimiento de las misiones y funciones propias de los mismos***.

A nivel local, la Legislatura de la CABA sancionó la Ley 1845 de PDP, cuyo objeto es la regulación de los datos personales en su jurisdicción de los bancos de datos públicos para garantizar el derecho al honor, la intimidad y la autodeterminación informativa según el art. 16 de la Constitución CABA. A su vez se prevé que también están incluidos dentro del sector público de la Ciudad todos los archivos o bases de datos de titularidad de los órganos de la administración, entes autárquicos, empresas y sociedades del estado, y otras organi-

zaciones empresariales, el poder legislativo y del judicial en cuanto a su actividad administrativa. En este sentido, el art. 22 dispone que será la Defensoría del Pueblo de la CABA el órgano de control de dicha ley y crea en su órbita el Centro de Protección de Datos con el Registro de Datos Personales, donde los ciudadanos podrán presentar sus reclamos de conformidad con el art. 4 inc. 3 de dicha ley y se garantizará el acceso a la información contenida en su registro. La citada Defensoría podrá representar a los titulares de datos personales a fin de hacer efectivo su derecho de acceso, rectificación, bloqueo o supresión, y también elaborará informes sobre proyectos que de alguna manera tengan impacto en el derecho a la privacidad y protección de datos personales.

Por la Ley 5688<sup>11</sup> se implementa el Sistema Integral de Seguridad Pública de CABA, el art. 17 dispone que es un deber de la Ciudad promover la efectiva participación ciudadana en asuntos de seguridad pública y el art. 483 hace referencia a que la instalación de sistemas de video vigilancia por parte del Poder Ejecutivo procede en la medida que resulte para una *utilidad concreta para adoptar medidas de gobierno relacionadas con el espacio público, limitando por el art. 484 la utilización de estos sistemas para tomar imágenes del interior de propiedades privadas salvo autorización judicial expresa pudiendo instalarse dispositivos en espacios públicos salvo cuando se afecte la intimidad de las personas.*

Así las cosas, según las constancias de la causa se verificó que el SRFP cuyo objetivo es la identificación y el reconocimiento de personas prófugas de la Justicia, está basado en el análisis en tiempo real de imágenes de video y que *salvo orden judicial se encuentra prohibido incorporar imágenes-datos biométricos y/o registros de personas que no se encuentren registradas en el CONARC.* Entonces la actualización diaria de la CONARC recoge altas y bajas y esa base de datos macheada con el RENAPER y trae los registros de CONARC.

Sin embargo, de la inspección realizada y del informe de la Defensoría surgió que este SRFP no fue auditado internamente, ni en la implementación ni en la aplicación.

La Defensoría del Pueblo como órgano de control de protección de datos personales y como auditora del SRFP no ha podido actuar, la

---

11 Ley 5688 disponible online en <http://www.sajj.gob.ar/LPX0006421> al 1/11/2022

Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia no está constituida, la Legislatura no puede verificar como funciona dicho sistema, el Ministerio de Justicia y Seguridad no efectuó una auditoria interna, dichas auditorias no son reemplazables por una auditoria de la Universidad de La Plata. Tampoco se dio cuenta del relevamiento de la infraestructura de red y servicios, ni de los procedimientos asociados a la aplicación y de la evaluación de mejores prácticas y generación de resultados.

***Todo lo antes dicho demuestra que este SRFP se implementó sin garantizar que cuente con los organismos de control que la Ley establecía, contrariando el principio de legalidad del accionar administrativo.***

Se comprobó que los errores y falencias producidas por el SRFP afectan directamente los derechos de las personas y la ausencia de los controles para su debida implementación implican un grave riesgo para vulnerar los datos personales y los derechos a la autodeterminación informativa, privacidad e intimidad.

Sumado a lo antes dicho y clave para la resolución del caso fue la pericia informática llevada a cabo por la PSA confirmando las irregularidades advertidas:

***“...existió una migración en cantidades exorbitantes de datos biométricos desde el RENAPER al MJYS CABA y a la Policía CABA a efectos de carga y alimentación del SRFP. Casi 10 millones de registros existentes en los archivos emitidos por el RENAPER responden a consultas efectuadas por dicho Ministerio”.***

***“...15459 personas fueron cargadas en el SRFP para ser buscadas sin encontrarse dentro de la base de CONARC, sin existir pedido de la justicia que habilite el accionar, sin sustento legal”***

***“...los datos biométricos de personas no requeridas judicialmente, fueron utilizados para alimentar y posteriormente ser ejecutados por el SRFP, existiendo búsquedas respecto de personas sin que se haya identificado el juzgado que las habría solicitado”.***

Es decir, que se constató todo lo descripto en contra de lo previsto por el art. 485 bis cuando determina que: “el SRFP será empleado únicamente para tareas requeridas por el Poder Judicial de la Nación, Provincial o de CABA como así también para la detección de personas buscadas exclusivamente por orden judicial registradas en la base de datos de CONARC. Salvo orden judicial se encuentra prohi-

bido incorporar imágenes, datos biométricos o registros de personas que no se encuentre registrados en CONARC”.

Es irrazonable que en materia de datos personales existan 17 distintos usuarios con el rol de administrador que no pueden ser vinculados a personas humanas que pueden acceder, tratar y eliminar datos biométricos de millones de personas.

Se hace una diferenciación entre el borrado lógico como procedimiento automático para estos sistemas y por el otro el físico, manual, voluntario y definitivo, se verificó que 356 registros de personas cuyos datos biométricos fueron incorporados al motor de búsqueda del SRFP fueron eliminados voluntaria y manualmente (borrado físico). Dichas personas se buscaron por el SRFP y la verificación de su motivo o justificación es imposible de saber porque sus registros se suprimieron de forma manual. Para este tipo de sistemas y en miras a un correcto resguardo de los datos personales el borrado físico debe ser inexistente porque dichas operaciones no pueden ser rastreadas afectando la trazabilidad de lo hecho.

La sentencia de la magistrada actuante en la Jurisdicción Contencioso Administrativa de 1° Instancia determinó que existe una afectación negativa a los derechos constitucionales cuya protección está garantizada a nivel local, por lo que declaró su inconstitucionalidad y el SRFP sólo podrá volver a implementarse una vez cumplidos todos los recaudos previos necesarios enumerados con anterioridad. En esa misma línea, como antecedente en el año 2009, la CSJN en el fallo Halabi indicó que cuando la dificultad para separar los “datos de tráfico” del contenido mismo de la comunicación y el riesgo cierto de que los datos registrados sean indebidamente utilizados con fundamento en la discrecionalidad de la Administración, deviene necesario un pronunciamiento como el comentado.

Cabe concluir que en un Estado democrático y constitucional de derecho, que se precie como tal, ninguna autoridad pública puede en uso de sus facultades avasallar y lesionar los derechos de los ciudadanos de esta manera, e implementar un sistema de IA sin parámetros de respaldo, que eviten riesgos innecesarios y que viole derechos humanos como la autodeterminación informativa, la privacidad y la protección de datos personales estando en juego garantías fundamentales no sería lo más aconsejable. Nadie puede negar que la utilización de IA en las actividades del Estado y en las actividades privadas de la vida diaria de las personas traen innumerables beneficios, pero corresponde hacer el planteo de a que costo,

o a riesgo de que derechos perder. Las evaluaciones de impacto sobre protección de datos personales brindan una herramienta teórico-práctica idónea que sirve para realizar este proceso o protocolo de razonabilidad, para determinar la proporcionalidad de medio a fin, el tema es hacer de su uso una obligación y no una mera facultad o recomendación. Los órganos de control de protección de datos personales a nivel regional y europeo así lo indican<sup>12</sup>, no sólo hay que replicar legislación en la materia sino aplicarla y hacer que se cumpla, este fallo es un claro ejemplo de ello.

Hago propias las reflexiones de CALVO P.<sup>13</sup>, debe reconocerse el potencial de las IA en el desarrollo y mejora de los sistemas democráticos, pero propuestas o políticas públicas como el SRFP adolecen de una reflexión previa sobre los problemas y las consecuencias negativas a la aplicación acrítica de estos sistemas. Es decir, que el camino debe hacerse al andar, y debe llevarse a cabo con un trabajo multidisciplinario de investigación y evaluación de impacto que minimice los efectos negativos y potencie los positivos en un escenario de transparencia y participación.

---

12 Ver casos Mercadona, Vodafone, BBVA aplicación de sanción y multas disponibles online en <https://civio.es/el-boe-nuestro-de-cada-dia/2022/02/22/vodafone-bbva-edp-y-mercadona-las-empresas-con-mayores-multas-por-incumplir-las-normas-de-proteccion-de-datos/> y <https://www.xataka.com/privacidad/reconocimiento-facial-mercadona-acaba-multa-2-5-millones-euros-que-dice-agencia-proteccion-datos-que-lecciones-se-pueden-extraer> al 1/11/2022

13 CALVO, P (2019) Democracia algorítmica: consideraciones éticas sobre la dataficación de la esfera pública, disponible online en <https://www.redalyc.org/journal/3575/357560862001/html/> al 1/11/2022.

**BIBLIOGRAFÍA**

Fallo de 1° Instancia Jueza Liberatori, SENTENCIA, 7 de Septiembre de 2022, JUZGADO EN LO CONTENCIOSO ADMINISTRATIVO Y TRIBUTARIO NRO 4. CIUDAD DE BUENOS AIRES, CIUDAD AUTÓNOMA DE BUENOS AIRES, Magistrados: Elena Amanda Liberatori disponible online [http://www.saij.gob.ar/FA22370014?utm\\_source=newsletter-semanal&utm\\_medium=email&utm\\_term=semanal&utm\\_campaign=jurisprudencia-provincial](http://www.saij.gob.ar/FA22370014?utm_source=newsletter-semanal&utm_medium=email&utm_term=semanal&utm_campaign=jurisprudencia-provincial) al 1/11/2022

Fallo Halabi Halabi, Ernesto c/ P.E.N. - ley 25.783 - dto. 1563/04 s/ amparo ley 16.986 disponible online en <http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-halabi-ernesto-pen-ley-25783-dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009-0ots-eupmocsollaf> al 1/11/2022

Ley 25326,

Reglamento Europeo PDP,

Guia para la Evaluación de Impacto en DP (Arg)

Directrices Éticas para una IA fiable- Grupo independiente de expertos de alto nivel sobre IA Comisión Europea.

Requisitos mínimos de seguridad de la información para los organismos del sector público nacional (Arg.)

Política Modelo de PDP para organismos públicos (Arg)

Derecho comparado:

Caso Mercadona Barcelona:

<https://www.xataka.com/privacidad/reconocimiento-facial-mercadona-aca-ba-multa-2-5-millones-euros-que-dice-agencia-proteccion-datos-que-lecciones-se-pueden-extraer>

[https://www.eldiario.es/politica/justicia-impide-mercadona-use-reconocimiento-facial-detectar-clientes-orden-alejamiento-tiendas\\_1\\_8025896.html](https://www.eldiario.es/politica/justicia-impide-mercadona-use-reconocimiento-facial-detectar-clientes-orden-alejamiento-tiendas_1_8025896.html)