Boletín de Jurisprudencia
**Diciembre 2023**

# NUEVAS TECNOLOGÍAS Y DERECHO:

## La judicialización de los sistemas de reconocimiento facial

ESCUELA DE LA DEFENSA PÚBLICA
MPD Argentina
O.D.I.A. OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO

**ÍNDICE**

## Escuela de la Defensa Pública de la Defensoría General De La Nación

El Ministerio Público de la Defensa de la Nación es una institución del sistema de justicia nacional y federal que se encarga de la defensa y protección de los derechos humanos. El MPD garantiza el acceso a la justicia y la asistencia jurídica integral, en casos individuales y colectivos, en especial de quienes se encuentren en situación de vulnerabilidad. La Constitución Nacional, en su artículo 120, instituye el MPD como un órgano independiente del resto de los poderes del Estado, con autonomía funcional y autarquía financiera. La Escuela de la Defensa Pública es responsable de las actividades de formación, actualización y perfeccionamiento que se realizan en el Ministerio Público de la Defensa. Su proyecto pedagógico se apoya en el empleo de diferentes estrategias; entre ellas, gestiona un ecosistema profesional en el que promueve la circulación y la producción de información jurídica con perspectiva de derechos humanos. En ese marco, el presente repositorio pone a disposición de toda la comunidad la selección y recopilación de jurisprudencia y otros materiales jurídicos producidos por el Ministerio Público de la Defensa.

## Observatorio de Derecho Informático Argentino (O.D.I.A.)

El Observatorio de Derecho Informático Argentino (O.D.I.A.) es una asociación civil sin fines de lucro. Fue creada con el objetivo de promover el ejercicio responsable de la ciudadanía digital y garantizar que los derechos de la comunidad sean respetados. O.D.I.A. lleva adelante trabajos de investigación, difusión, capacitaciones y litigio estratégico. Cuenta con profesionales del mundo del derecho y de la informática, y también personas provenientes de diferentes ámbitos interesadas en el cruce del derecho y de las tecnologías de la información. La interdisciplinariedad es un eje central al momento de investigar con rigurosidad técnica aquellas situaciones derivadas del uso de nuevas tecnologías y cómo afectan la vida cotidiana de las personas.

# INTRODUCCIÓN

*Escuela De La Defensa Pública*

*Defensoría General De La Nación*

El boletín "Nuevas tecnologías y derecho: La judicialización de los Sistemas de Reconocimiento Facial" fue elaborado entre la Escuela de la Defensa Pública de la Defensoría General de la Nación y el Observatorio de Derecho Informático Argentino (O.D.I.A.). Asimismo, para el trabajo sobre esta temática contamos con la participación especial de Antonella Bentín, Secretaría de Primera Instancia de la Defensoría Pública Oficial Federal de Concordia, provincia de Entre Ríos.

Este trabajo recopila jurisprudencia nacional e internacional y diferentes documentos de interés sobre el uso e implementación de los Sistemas de Reconocimiento Facial. La jurisprudencia analizada pone en relieve que la implementación y utilización de estos sistemas en condiciones precarias y sin el control suficiente entran en tensión con los derechos y garantías de los ciudadanos. Por otro lado, los documentos de interés tienen por objetivo contribuir a la comprensión de estas nuevas tecnologías.

En cuanto al recorte temporal y espacial del análisis que se propone, se analizaron cuatro sentencias nacionales y cinco internacionales de diferentes tribunales y jurisdicciones, dictados entre 2019 y 2023. El criterio de selección estuvo basado en poder recoger la mayor cantidad de pronunciamientos en una temática novedosa y poco explorada a nivel nacional. Toda la información se encuentra enlazada a la base de conocimientos del área, donde se puede consultar el texto completo.

En atención a que es posible que existan pronunciamientos referidos a esta temática que no se encuentren incluidos en este boletín, solicitamos que por favor nos escriban un correo electrónico a jurisprudencia@mpd.gov.ar en caso de que se haya omitido jurisprudencia cuya incorporación pudiera resultar relevante.

# PALABRAS INICIALES. DERECHO Y TECNOLOGÍA: NUEVAS TENSIONES

*Observatorio de Derecho Informático Argentino (O.D.I.A.)*

En el complejo entramado de la sociedad digital contemporánea, la creciente intermediación tecnológica en nuestros ejercicios cívicos comienza a plantear una desafiante dualidad. Por un lado, las promesas de seguridad y eficiencia, representadas en las nuevas tecnologías, emergen como demandas ciudadanas en procura de solucionar demandas históricas. Sin embargo, al mismo tiempo, el desarrollo de estos elementos muestra señales cada vez más claras sobre sus riesgos para la salvaguarda de los Derechos Fundamentales sobre los que nuestras sociedades han pretendido estructurarse. Este nuevo escenario ha dado lugar a una nueva puja bifronte plagada de posiciones con argumentos, supuestamente, antagónicos entre, por un lado, quienes bregan por una la implementación de soluciones técnicas y, por el otro, aquellos que pretenden la salvaguarda de las normas constitucionales como condición necesaria.

Si bien poca novedad presentaría la existencia de un debate en estos términos, este nuevo escenario se encuentra singularizado por el alto grado de analfabetismo digital existente. Aun cuando la intermediación tecnológica se torna cada vez más ubicua, la inmensa mayoría de la ciudadanía carece de elementos teóricos esenciales que permitan comprender nociones elementales como, por ejemplo, el funcionamiento de Internet. Tal realidad dota en nuestra vida actual de un inédito grado de opacidad a las herramientas que conforman nuestros entornos cotidianos de existencia. Esta situación, lejos de significar una situación alarmante en cuanto a las relaciones de carácter privado, como podrían ser las de consumo, constituye también una sustancial alteración de las posibilidades de control y defensa de nuestros derechos frente a las herramientas informáticas que sustentan nuestra cotidianidad. Al respecto, cabe señalar que este desconocimiento técnico y opacidad informática resulta una realidad que atraviesa de modo transversal a los distintos estamentos sociales y está presente, incluso, entre las propias autoridades públicas.

Recientemente, las controversias en torno al uso de la inteligencia artificial (IA) han emergido como una temática central en la definición de estándares que posibiliten la defensa de nuestros Derechos Fundamentales[1]. Dentro de este conjunto de herramientas automatizadas, el uso de Sistemas de Reconocimiento Facial (SRF) en espacios públicos ha ocupado un lugar central en los desarrollos normativos y jurisprudenciales actuales contemporáneos.[2] Esta realidad, ha impuesto

[1] En este sentido, ver la "Declaración de Montevideo sobre Inteligencia Artificial y su impacto en América Latina"; las "Orientaciones mundiales sobre la IA Generativa en la Educación y la Investigación" elaborada por la UNESCO; y la Carta Abierta para pedir que se detenga la implementación de las nuevas inteligencias artificiales durante seis meses.

[2] Véase el Proyecto de Ley para regular la IA elaborado por el Parlamento Europeo.

a las distintas contiendas sobre la implementación de los SRFs como antecedentes de peso en la conformación de una visión que posibilite la defensa de los Derechos Constitucionales ante la creciente intermediación tecnológica.

## Video vigilancia, imágenes y uso de Sistemas de Reconocimiento Facial (SRF) en procesos sancionatorios

Este boletín presenta dos casos en los que se utilizaron SRF para identificar al acusado: el caso "Glukhin v. Rusia" del Tribunal Europeo de Derechos Humanos y el caso "State of New Jersey v Francisco Artega", resuelta por el Superior Tribunal del Estado referido.

En "Glukhin v. Rusia", si bien no se trató de un caso criminal, ya que la persona fue juzgada por la comisión de una falta administrativa y, por lo tanto, no se trataron cuestiones relativas a la afectación de garantías propias del proceso penal, sí se cuestionó el uso de tecnologías de reconocimiento facial. Tal línea argumentativa sirve para pensar cuestiones propias del proceso penal. Las circunstancias relevantes del caso pueden resumirse de la siguiente manera: un hombre realizó una manifestación pacífica en un subterráneo de Moscú sin cumplir con una notificación administrativa previa requerida por ley. A partir de imágenes que circularon en redes sociales y el sistema de vigilancia del subterráneo, la policía rusa utilizó SRF para dar con la persona. El acusado sostuvo que tal uso era ilegal porque la Ley de actividades de búsqueda operativa (la OSAA) no autorizaba el uso de tecnologías de reconocimiento facial para investigar infracciones administrativas. El tribunal local lo condenó al pago de una multa. Al resolver, el TEDH resaltó que la utilización de sistemas de reconocimiento facial, en primer lugar, para identificarlo a partir de las fotografías y el video que habían sido publicados en Telegram y, en segundo lugar, para localizarlo y detenerlo posteriormente mientras viajaba en el subterráneo de Moscú, constituyó una injerencia en su derecho al respeto de su vida privada en el sentido del artículo 8, apartado 1, del Convenio (cfr. párr. 73). El Tribunal resaltó que "el uso de esas tecnologías exige una justificación de gran relevancia para ser considerada 'necesaria en una sociedad democrática' ya que podría tener un efecto amedrentador ('*chilling effect*') respecto a los derechos a la libertad de expresión y asociación" (cfr. párr. 88).

Conviene recordar que, en el 2018, en el ámbito de la CABA, se discutió la incorporación en el Código Procesal Penal local un capítulo especial referido a sistemas de vigilancia electrónica como medidas de investigación. El tratamiento de ese capítulo generó fuertes críticas por partes de

varios legisladores[3] y ONGs[4] al punto que fue eliminado para lograr consenso en otras modificaciones. Lo interesante es que los argumentos expuestos en esa oportunidad, a grandes rasgos, son similares a los enunciados por el Tribunal Europeo, y los temores expuestos parecieran confirmarse con el uso del SRF en la CABA.

Pero, volvamos a uno de los argumentos esgrimidos por el acusado en el caso ruso: él sostuvo que la utilización del SRF en el proceso era ilegal. ¿Se podrían utilizar SRF y, consecuentemente, valerse de la información reunida para ser presentada en un proceso penal -o contravencional- en nuestro país a pesar de no estar reglamentados por ley? ¿El acusador puede valerse del principio de libertad probatoria para fundar la admisión de dicha información como prueba en un juicio oral?

Entre estas dos preguntas oscilan las opiniones en torno al uso de los SRF y la validez de la información producida en el marco de una investigación penal. Las dos preguntas pueden ser pensadas como una re escenificación de dos modelos en pugna: control y persecución del delito por sobre derechos y garantías, frente a un modelo de debido proceso legal que pone en primer lugar el respeto a las garantías constitucionales. O, puesto en términos jurídicos, que toda disposición legal que coarte la libertad personal o que limite un derecho debe ser interpretada restrictivamente; frente a aquella que consagra la libertad probatoria al admitir que podrán acreditarse por cualquier medio de prueba los hechos o circunstancias de interés para la solución del caso.

Ante la falta de reglamentación legal, algunos dirán que bastará con conseguir una autorización judicial para tornar legítimo el uso y requerir la admisión a juicio de la información reunida. Al admitir el principio de libertad probatoria en este sentido, aceptan la idea según la cual, en

[3] Los legisladores Roberto, Heredia y Gottero señalaron que las nuevas medidas de investigación: "alcanzan un nivel preocupante ya que consideramos que este tipo de medidas deben ser excepcionales y solo utilizarse en la persecución de los delitos más graves. De aprobarse este proyecto de reforma se podrían aplicar a delitos menores e, inclusive, a la investigación de contravenciones" (Observación al Despacho Nº 642). Los legisladores Bregman y Del Corro se centraron en advertir los posibles usos ilegales de estas nuevas herramientas de investigación por parte del Estado contra las organizaciones sociales, gremiales, de la izquierda y de la oposición en su conjunto. Consideraron que estas nuevas medidas de investigación conceden un mayor poder de actuación a la Policía de la Ciudad, que a partir de "(…) ahora será la responsable de realizar espionaje e infiltraciones. El armado de causas y el espionaje quedan legalizados y sin control (Observación al Despacho Nº 642).

[4] Un colectivo de organizaciones no gubernamentales firmó una carta dirigida a la Comisión de Asuntos Penales y Constitucionales de la Legislatura de la Ciudad e instaron a los legisladores a dejar sin efecto la incorporación de las medidas especiales de investigación Las organizaciones firmantes del documento fechado el 28 de septiembre de 2018 fueron las siguientes: Access Now; Amnistía Internacional Argentina AI; Asociación Civil por la Igualdad y la Justicia ACIJ; Asociación por los Derechos Civiles ADC; Asociación Pensamiento Penal Capítulo Buenos Aires APP; Centro de Estudios Legales y Sociales CELS; Centro de Estudios en Libertad de Expresión y Acceso a la información CELE; Colectivo para la Diversidad COPADI; Fundación Vía Libre; Instituto de Estudios Comparados en Ciencias Penales y Sociales INECIP y Poder Ciudadano.

materia procesal penal, resulta admisible la aplicación analógica de las normas que regulan los medios de prueba, aun cuando pudieran afectar derechos del imputado.

Pero, ¿por qué tenemos que ser menos exigentes con la utilización en el proceso de nuevas tecnologías cuya real afectación muchas veces no resulta del todo dimensionada; por qué ser laxos en regulación de nuevos medios de prueba, basados en tecnologías cuyo funcionalidad y operatividad desconocemos en profundidad? ¿Y por qué los jueces pueden permitirse una mayor flexibilidad con respecto a estas nuevas tecnologías, potencialmente más invasivas de la intimidad que los tradicionales?

A nuestro entender, se necesita contar con una reglamentación legal, estricta y previa[5] para la utilización de SRF en el proceso penal o cualquier otro proceso que implique la imposición de una sanción. En este punto resultan ilustrativas las consideraciones de Pérez Barberá acerca de la aplicación de nuevas tecnologías en el proceso penal: "…*las investigaciones que actualmente se llevan a cabo en Argentina mediante rastrillajes informáticos, intervenciones de e-mails, seguimiento de direcciones IP, grabaciones o filmaciones a distancia, etc., resultan inconstitucionales (sin perjuicio de la salvedad que quepa realizar respecto de la ley de estupefacientes). Pues tales medios de prueba no han sido previstos en las leyes procesales, y en consecuencia su utilización para fortalecer la hipótesis acusatoria (es decir: para perjudicar procesalmente al imputado) constituye una aplicación de la ley procesal penal por analogía in* malam partem *y, por lo tanto, contraria al principio de legalidad penal, que rige con toda su amplitud tanto en el derecho penal material como en el derecho procesal penal*".[6]

Por su parte, el caso "Arteaga" sí es un caso criminal. A grandes rasgos, los hechos del caso fueron los siguientes: un "hombre hispano con gorro de lana negro" ingresó a una tienda con un arma y robó dinero. A partir de las imágenes de las cámaras de vigilancia de la tienda y de una propiedad cercana generaron una imagen fija y la enviaron al Centro Regional de Inteligencia de Operaciones (NJROIC) de Nueva Jersey para reconocimiento facial. Un investigador de NJROIC informó que no había coincidencias, pero podía volver a "correr" la búsqueda si los detectives le proporcionaron una mejor imagen. No consiguieron una mejor imagen y, en cambio, los detectives enviaron todas las imágenes de vigilancia sin editar al Servicio de Identificación Facial del Departamento de Policía de Nueva York "Real time crime center" (NYPDRTCC). Un detective capturó una imagen fija del metraje y la comparó contra las bases de datos del centro y ofreció al acusado como una "posible coincidencia". Finalmente, los detectives que trabajaron en el caso en Nueva Jersey crearon dos series fotografías diferentes, compuestas por cinco fotografías de relleno y la fotografía que NYPD RTCC proporcionó, se las exhibieron a las dos testigos del caso que eran empleadas de la tienda y reconocieron al sujeto de la imagen como autor del hecho.

[5] "En consecuencia, toda actividad procesal destinada a destruir el estado de inocencia constitucional que protege al imputado deberá estar previamente regulada en ley, y de modo estricto, claro y taxativo, pues, en definitiva, de dicha actividad dependerá la eventual imposición de una pena. La aplicación analógica de la ley procesal con la finalidad de posibilitar la condena del imputado queda, pues, vedada". Pérez Barberá, Gabriel. 2009. "Nuevas tecnologías y libertad probatoria en el proceso penal", en Nueva Doctrina Penal, 2009/A, p. 277.

[6] Ibidem, p. 280.

El caso llegó a la Corte porque el juez de juicio le denegó a la defensa su moción para obligar al Estado —a través del "*Discovery*"— a proporcionar pruebas relacionadas con la tecnología de reconocimiento facial (FRT) utilizada.

En el caso se discutió la aplicación de la regla "Brady ("Brady v. Maryland) —la cual impone al estado la obligación de proporcionar a la defensa la evidencia o información exculpatoria o favorable al acusado para garantizar el debido proceso— para que en los términos del Discovery solicitado se le entrega a la defensa información relativa al SRF empleado para poder preparar su defensa. Entre los trece puntos solicitados, se encontraban: el nombre y fabricante del software de reconocimiento facial utilizado; el código fuente del algoritmo(s) reconocimiento facial; las tasas de error del sistema; el rendimiento/performance de/los algoritmo(s) utilizados en las "pruebas de proveedores de reconocimiento facial que aplica el NIST [National Institute of Standars and Technology]; una lista o descripción del número de rango o puntuaciones de confiabilidad producidas por el sistema, incluyendo la escala en la que se basa el sistema.

La Corte consideró que en el caso correspondía aplicar la Regla Brady porque las pruebas buscadas estaban directamente relacionadas con la capacidad de la defensa para probar la confiabilidad del SRF y, en consecuencia, para impugnar la identificación realizada por los testigos, crear dudas e incluso demostrar la posible culpabilidad de un tercero. Concluyeron que, sin ninguna información sobre la confiabilidad del SRF, no podía haber un juicio justo, en especial si los frutos de ese uso de la tecnología son admitidos como evidencia. Por ello, ordenaron al juez de juicio cumplir con todos los puntos del *discovery* solicitado por la defensa.

Los derechos no son nunca el resultado automático de los mecanismos de garantía formalmente previsto en las constituciones. Los derechos: "…se desarrolla(n) en un determinado contexto histórico-social e histórico-político, que condiciona de manera decisiva su efectividad práctica. En concreto, cada tiempo histórico produce su propia cultura de los derechos, privilegiando un aspecto respecto a otro o poniendo las libertades en su conjunto más o menos en el centro del interés general"[7].

Ya adentrados en el siglo XXI, es momento de generar nuestra propia cultura de derechos y garantías en un ecosistema digital, que reconozca el desafío de pensar, controlar y legislar de manera pormenorizada el uso de nuevas tecnologías, en especial, los SRF, respecto de las cuales desconocemos su lógica y funcionamiento interno; y para el caso de su uso en investigaciones criminales, reglamentar en los códigos de procedimiento tanto las medidas de investigación que implican su uso con fines de vigilancia como los medios de prueba destinados a la obtención de la prueba digital.

O.D.I.A.
Observatorio de Derecho Informático Argentino
https://odia.legal/
@ODIAasoc

[7] Fioravanti, Mauricio (2007);" Los derechos fundamentales", p. 24.

# 1. JURISPRUDENCIA NACIONAL

## 1.1. CÁMARA DE APELACIONES EN LO CONTENCIOSO, ADMINISTRATIVO, TRIBUTARIO Y DE RELACIONES DE CONSUMO. SALA I. SECRETARÍA ÚNICA. "OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.)". EXPEDIENTE N° 182908/2020. ACTUACIÓN N° 1565405/2021. 11/8/2021.

**HECHOS**

El Gobierno de la Ciudad de Buenos Aires implementó el Sistema de Reconocimiento Facial de Prófugos (SRFP) en la jurisdicción de Ciudad Autónoma de Buenos Aires. El SRFP buscaba determinar si los rostros que se obtenían mediante el uso de cámaras de videovigilancia se encontraban y si correspondían o no con los rostros almacenados en la base de datos del sistema de Consulta Nacional de Rebeldía y Capturas (CoNaRC).

El Observatorio de Derecho Informático Argentino (O.D.I.A) promovió una acción de amparo con el objetivo de cuestionar la constitucionalidad de la Ley N° 6339 y de la resolución N° 398/MJSGC/19, mediante los cuales se había implementado el SRFP. Para ello, sostuvo que el Gobierno de la Ciudad de Buenos Aires había contratado el uso e implementación del Sistema de Reconocimiento Facial de forma directa con una empresa privada sin un debate previo que permita sostener su pertinencia y seguridad. Además, señaló que los efectos de la vigencia de esa normativa lesionaban de forma manifiesta los derechos de toda la sociedad. También precisó que las bases de datos de las caras que luego serán comparadas tienen predominancia de hombres blancos cisgénero, por lo que los sistemas de reconocimiento facial aprenden mejor cómo diferenciar a dos personas con estas características que al resto de la población y por ello la mayoría de esos programas suelen presentar sesgos en cuanto discriminan por raza, color y etnia.

El juzgado N° 11 de primera instancia en lo Contencioso, Administrativo y Tributario rechazó *in limine* la acción de amparo interpuesta. Para decidir así, indicó que la actora pretendía un pronunciamiento judicial en abstracto acerca de la adecuación legal y constitucional la Ley N° 6339 y de la resolución N° 398/MJSGC/19 y que no se había cuestionado ningún acto u omisión sustentados en esas normas. Destacó que no se había planteado un caso concreto particular en el que se hayan visto afectados los derechos invocados ni tampoco era posible visualizar la amenaza a esos derechos en abstracto sin caer en el campo de lo hipotético. En esa línea, mencionó que O.D.I.A. no alegó ni intentó probar la existencia de un daño particular y que únicamente buscaba sanear la supuesta inconformidad de la normativa impugnada. Además, explicó que no se trataba de una acción que buscara la protección o tutela de derecho difusos, sino que involucraba la tutela de derechos subjetivos individuales, cuya protección era exclusiva de sus titulares mediante acciones individuales, o colectivas promovidas por el colectivo de personas afectadas o por asociaciones que las representaran. Concluyó que lo que pretendía la actora podía ser canalizado, al menos en el ámbito de la Ciudad de Bueno Aires, a través de una acción declarativa de inconstitucionalidad ante el Tribunal Superior de Justicia de la Ciudad de Buenos Aires. Contra esa decisión O.D.I.A. interpuso un recurso de apelación.

**DECISIÓN**

La Sala I de la Cámara de Apelaciones en lo Contencioso, Administrativo, Tributario y de Relaciones de Consumo de la Ciudad de Buenos Aires hizo lugar al recurso de apelación y revocó la sentencia del juzgado de primera instancia.

ARGUMENTOS

1. **Sistema de Reconocimiento Facial. Procesos colectivos. Acción de amparo. Derechos de incidencia colectiva. Control de constitucionalidad. Rebeldía.**

"[E]n autos no se pretende que el tribunal ejerza un control de constitucionalidad en abstracto, propio del sistema concentrado (artículo 113, inciso 2° de la Constitución local). Antes bien, la actora da cuenta de circunstancias puntuales que, según postula, importarían una amenaza concreta a derechos de incidencia colectiva. Así las cosas, la situación descripta en el escritorio de inicio justifica la intervención de los tribunales del fuero y el ejercicio por su parte del control de constitucionalidad difuso; que es resorte —como ya se señaló— de todos y cada uno de los jueces llamados a resolver los casos que se les presenten".

"[E]n la presente controversia la pretensión se refiere a los efectos comunes de la conducta estatal cuestionada: la puesta en marcha del Sistema de Reconocimiento Facial que se habría efectuado sin el debido debate acerca de la pertinencia y seguridad del sistema, en tanto ello pondría en peligro derechos constitucionales, en especial la garantía de no discriminación, como así también los derechos a la privacidad, la intimidad y la protección de datos personales, entre otros. En este sentido, la asociación actora sostuvo que el GCBA no había realizado la correspondiente evaluación del impacto en la privacidad (EIP), que sí realizaron otros países a fin de determinar la justificación, legitimidad, necesidad y proporcionalidad del uso del sistema, razón por la cual no es sería posible determinar el impacto y la posible afectación a los datos personales y otros derechos humanos básicos de los ciudadanos de la CABA.

La presunta lesión tendría su origen en un hecho único y complejo (la sanción de la Ley N.º 6339, el dictado de la Resolución N.º 398/MJYSGC/19 y la puesta en marcha del Sistema de Reconocimiento Facial creado por dichas normas), que podría afectar a los ciudadanos que —al circular— son captados por las cámaras del Sistema de Reconocimiento Facial de prófugos".

"[E]l proceso colectivo incoado es susceptible de potenciar la celeridad y eficacia de la respuesta judicial y, además, no se aprecia que la legitimación así admitida colisione —es decir, resulte incompatible— con la que atribuida singularmente a cada ciudadano que se considere afectado por la implementación del sistema o, en caso, por sufrir un perjuicio concreto a raíz del mismo (por caso, una persona detenida o demorada por errores en el sistema por un falso positivo en la detección de rostro).

[E]l texto constitucional local y las circunstancias de la causa enunciadas permiten sostener que no se trata de derechos puramente individuales y exclusivos de cada uno de los titulares afectados, sino que se persigue la tutela de un derecho de incidencia colectiva referente a intereses individuales homogéneos —en especial, el derecho a la no discriminación—".

**2. Sistema de Reconocimiento Facial. Acción de amparo. Procesos colectivos. Legitimación.**

"Entonces, de la letra expresa del acta [de constitución de la asociación civil O.D.I.A.] surge que la asociación actora tiene entre sus fines la defensa de los intereses de toda la ciudadanía del territorio argentino y su representación en post de garantizar el adecuado ejercicio de los derechos constitucionales tanto individuales como colectivos.

Es con sustento en estos objetivos que la demandante se encuentra legitimada como parte actora en esta causa, ya que la convicción de reclamar el respeto al derecho a la no discriminación, como así también proteger el derecho a la intimidad, a la privacidad, a la protección de los datos personales, entre otros, importa ejercer la defensa plena de los derechos de las personas cuyas imágenes podrían ser captadas por las cámaras del Sistema de Reconocimiento Facial de prófugos —sistema cuya validez constitucional se discute en autos—.

Todo lo hasta aquí señalado resulta concordante con la legitimación particularmente amplia que el art. 14 de la Constitución local confiere a cualquier habitante y a las personas jurídicas defensoras de derechos o intereses colectivos frente a la discriminación o la afectación de derechos o intereses colectivos".

**3. Sistema de Reconocimiento Facial. Acción de amparo. Procesos colectivos. Derechos de incidencia colectiva. Igualdad. No discriminación. Control de constitucionalidad.**

"Así pues, más allá de si asiste o no razón a la actora en su pretensión de fondo (cuestión que, en atención a la etapa procesal en que se encuentra el presente proceso, aún no puede ser determinada), lo cierto es que, entre otros derechos, en su demanda invoca expresamente el derecho a la no discriminación [...]. En ese orden, plantea la problemática relativa a la existencia de sesgos discriminatorios en sistemas de reconocimiento facial como el implementado por la demandada; sesgos que, según postula, resultan particularmente gravosos para las minorías.

Se refiere, asimismo, a los falsos positivos a los que estaría expuesto el sistema y al modo en que ello afectaría los derechos de las personas alcanzadas por esos errores.

En suma, los términos en que ha sido planteada la acción permite[n] sostener que no se trata de una impugnación en abstracto, sino de un caso judicial en los términos del artículo 14 de la Constitución local, articulado por quien se encuentra legitimado para requerir la tutela de los derechos invocados, lo cual admite el control difuso de constitucionalidad por la vía intentada a fin de que el juzgador brinde la tutela pretendida por la demandante (ver considerando VII del presente).

Desde esta perspectiva, y teniendo en cuenta el carácter restrictivo con el que procede el rechazo *in limine* de la acción y el principio *pro actione*, la resolución impugnada debe ser revocada".

"[E]l planteo […] no se refiere a un cuestionamiento abstracto de una norma general que habilitaría la competencia originaria y exclusiva del Tribunal Superior de Justicia (artículo 113 inciso 2 ya citado), sino que, tal como fue dicho precedentemente, la parte actora ha invocado a los fines de su legitimación en defensa del interés de la sociedad cuestiones vinculadas con supuestos de discriminación como así también la vulneración a los derechos a la privacidad, la

intimidad y la protección de datos personales, entre otros, lo que cual resulta suficiente para acceder a la justicia (artículo 14 de la CCABA), a fin de que el juez le brinde una tutela individual ajena al cometido de la acción cuya competencia originaria ha sido confiada por la Constitución local al Superior Tribunal".

# 1.2. JUZGADO DE 1° INSTANCIA EN LO CONTENCIOSO, ADMINISTRATIVO Y TRIBUTARIO N° 2. SECRETARÍA N° 3. "OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.)". EXPEDIENTE N° 182908/2020. ACTUACIÓN N° 783420/2022. 11/4/2022.

**HECHOS**

El Gobierno de la Ciudad de Buenos Aires implementó el Sistema de Reconocimiento Facial de Prófugos (SRFP) en la jurisdicción de Ciudad Autónoma de Buenos Aires. El SRFP buscaba determinar si los rostros que se obtenían mediante el uso de cámaras de videovigilancia se encontraban y si correspondían o no con los rostros almacenados en la base de datos del sistema de Consulta Nacional de Rebeldía y Capturas (CoNaRC). Contra esa decisión, el Observatorio de Derecho Informático Argentino (O.D.I.A.) promovió una acción de amparo para que se suspenda su aplicación por considerar que afectaba, entre otros, el derecho a la libre circulación de las personas. Dentro de otras cuestiones, manifestaron que el sistema arrojaba casos de "falsos positivos" a partir de los cuales la policía detenía de manera errónea a personas que no tenían pedido de captura.

**DECISIÓN**

La Secretaría n°3 del Juzgado de 1° instancia en lo Contencioso Administrativo y Tributario n°2 de CABA hizo lugar a la medida cautelar solicitada y ordenó al Gobierno de la CABA suspender el Sistema de Reconocimiento Facial de Prófugos (SRFP) (juez Gallardo).

**ARGUMENTOS**

1. **Sistema de Reconocimiento Facial. Vigilancia electrónica. Política criminal. Registro Nacional de Reincidencia y Estadística Criminal y Carcelaria.**

"[E]l SRFP mediante las cámaras de video vigilancia capta imágenes que se visualizan y procesan en el Centro de Monitoreo Urbano (CMU) de la Policía de la Ciudad y las coteja con los datos biométricos contenidos en la CoNaRC, y en caso de advertir una coincidencia, emite una alerta para que personal policial actúe en consecuencia.

[E]l propio Director del Registro Nacional de Reincidencia (organismo dentro del que funciona la CoNaRC) sostuvo que ´se advierte que la utilización de esta base de datos puede motivar algún tipo de conflicto al dar lugar a una detención errónea comúnmente denominado ´falso positivo´´ y que ´no se ha suscripto ningún convenio con el Ministerio de Justicia y Seguridad de CABA ni con la Defensoría del Pueblo local´ […].

En el mismo informe, concluyó que ´la utilización de la CoNaRC, en el marco del Sistema de Reconocimiento Facial de Prófugos empleado en el ámbito de la Ciudad Autónoma de Buenos Aires, puede generar diferentes problemáticas, dado el funcionamiento del mismo, toda vez que a pesar de realizarse los pertinentes contralores y relevamientos permanentes de la información contenida en dicha base de datos, por parte de este Registro Nacional de Reincidencia, pueden surgir diferentes supuestos tales como, fallas en los datos patronímicos de las personas humanas

incluidas, fuere por información falsa brindada por la propia persona humana, o por errores involuntarios de parte de los operadores del sistema judicial; modificación de temperamentos procesales, cuya comunicación para su debida toma de razón, se demora por razones ajenas a este organismo; todo lo cual pudiere dar lugar a detenciones erróneas —falsos positivos— con las consecuencias disvaliosas que eso acarrearía al sujeto de derecho involucrado´ […]".

"Por otro lado, el único registro sobre el cual opera el SRFP, es decir la CoNaRC, poseería serias fallas que, en palabras del Director Nacional de Reincidencia, darían ´lugar a detenciones erróneas —falsos positivos— con las consecuencias disvaliosas que eso acarrearía al sujeto de derecho involucrado´.

Estas falencias en el sistema podrían conllevar que personas que se encuentren dentro del territorio de la Ciudad sean confundidos con prófugos de la justicia y detenidos por las fuerzas de seguridad […].

[E]l hecho de que los errores y/o fallas recaigan sobre la base de datos de la CoNaRC y no sobre el Sistema de Reconocimiento Facial de Prófugos en sí mismo no puede ser considerado como un argumento válido para soslayar los riesgos que entraña. Es que, de modo alguno el GCBA podría seriamente pretender ejecutar un sistema que por ley (artículo 485 bis de la ley 5..688) opera exclusivamente para detener personas registradas en la CoNaRC si aquella base de datos contiene falencias que puedan implicar el menoscabo de los derechos de los ciudadanos.

El sistema debe ser comprendido de modo integral, en su totalidad y no en forma compartimentada. Más allá de que la CoNaRC no se encuentre dentro de la órbita del GCBA, lo cierto es que en virtud de los efectos que trae aparejado el uso de esta base en el marco del SRFP, deben desarrollarse mecanismos de articulación concretos para eliminar situaciones que vayan en detrimento de los derechos de las personas.

[E]l propio Director [del Registro Nacional de Reincidencia] asumió que ´a pesar de realizarse los pertinentes contralores y relevamientos permanentes de la información contenida en dicha base de datos´ el sistema puede arrojar falsos positivos.

En ese contexto, es evidente la disfuncionalidad de un Estado que compartimenta su actividad para desentenderse voluntariamente de aquellas cuestiones que escapan a áreas específicas de determinada cartera, como si fuesen compartimentos estancos. Por el contrario, el paradigma actual exige medidas de acción positiva para intervenir directamente. Allí donde están los problemas, debe estar el Estado contribuyendo enérgicamente a una solución".

**2. Detención de personas. Principio de inocencia. Derecho al honor. Derecho a la intimidad.**

"[R]esulta sumamente lógico que previo a la creación e implementación de un Sistema de Reconocimiento Facial para la detención de personas, se realice una prueba o un estudio de su impacto sobre los derechos de ellas y se cree una base de datos específica sobre la cual opere. Máxime, cuando se trata de derechos protegidos constitucional y convencionalmente.

A su vez, toda la normativa relacionada con el tratamiento de datos personales requiere de una alta rigurosidad en busca de su protección integral, estén ellos asentados en archivos, registros,

bancos de datos, u otros medios técnicos de tratamiento de datos, tanto públicos como privados, para de este modo garantizar el derecho al honor, a la intimidad y el acceso a la información que sobre las mismas se registre".

"[Cobran] especial relevancia […] varios casos en los que personas fueron detenidas erróneamente como consecuencia de alertas impartidas por la utilización del SRFP, es decir, por falsos positivos. Dicha situación configuraría una detención arbitraria y atentaría contra el principio de inocencia".

**3. Autonomía. Principio de reserva. Participación pública. Derecho a la información.**

"La trascendencia del principio de privacidad es tal que sólo con ella es posible diseñar un sistema de respeto a la autonomía y a la libertad a la vez de establecer una frontera ante las atribuciones estatales para limitar los derechos. […] [E]s dable recalcar que el art. 19 de la Constitución Nacional y 12 de la Constitución Local delimita un ámbito cerrado a la intervención del Estado y de terceros, que el SRFP —a la luz de la información recolectada— cruzaría tal frontera y que podría generar un choque con la privacidad e intimidad de los ciudadanos de la CABA. Con relación a ello, [resulta] pertinente subrayar que el derecho a la intimidad debe ser entendido de modo amplio y omnicomprensivo. Comprende sencillas manifestaciones del derecho a la soledad y a no ser perturbado en la vida privada, como también otras situaciones, por ejemplo, la reserva y confidencialidad de ciertos actos, la intimidad familiar, la defensa del honor, el derecho a la propia imagen o la protección de la identidad [hay nota]".

"[L]a falta de creación de la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia y de convocatoria de la ciudadanía a debatir las cuestiones relativas al Sistema de Reconocimiento Facial de Prófugos colisionaría con la conducta participativa que imprime la normativa local. Ello en cuanto se habría privado tanto a habitantes, como legisladores y organizaciones especializadas, de intervenir conforme lo ordena la Constitución Local y la ley de Seguridad Pública a colaborar en la mejor decisión a adoptar respecto a la creación, funcionamiento e implementación del SRFP".

"[E]l hecho de no haber creado el registro prescripto en el artículo 495 de la ley 5.688 se daría de bruces con el principio de transparencia e información estadística contable establecidos en su artículo 9 y socavaría el derecho de información y de acceso reconocidos en los incisos a y b del artículo 13 de la ley local 1.845 respectivamente y artículo 6 de la ley nacional 25.326.

[T]ambién la falta de creación de la Comisión de la Legislatura vulneraría el derecho a la participación ciudadana reconocida constitucionalmente (artículo 34 CCABA) y como uno de los principios rectores en lo que respecta al Sistema Integral de Seguridad Pública de la CABA (artículo 9 de la ley 5.688)".

**4. Política criminal. Reglamentación de los derechos. Registro Nacional de las Personas. Rebeldía. Orden de captura. Principio de proporcionalidad.**

"[E]l listado remitido por el Ministerio de Justicia y Derechos Humanos de la Nación denota que las personas incluidas en la CoNaRC al 25/04/2019 eran aproximadamente 35.000 y al momento de la contestación del oficio ascendía a aproximadamente 40.000 registros (circunstancia que

coincide con lo informado mediante nota NO-2020-70688753-APNRNR#MJ). Mientras que según lo informado por el ReNaPer, las solicitudes de datos biométricos efectuadas por el GCBA entre el 25/04/2019 Y 20/12/2021 fueron 9.392.372 y entre el 21/12/2021 y el 09/03/2022 fueron 507.911. Esto es, un total de extracciones de 9.900.282 en menos de dos años, dentro de los que el SRFP se habría encontrado mayormente inactivo.

Resulta al menos alarmante la excesiva discordancia cuantitativa que se advierte entre el listado de personas suministrado por la CoNaRC, donde están registradas todas las personas declaradas en rebeldía, con capturas, averiguación de paradero y/o comparendos y las peticiones de datos biométricos efectuadas por el GCBA.

Lo hasta aquí verificado parece suficiente para poner de relieve la irregularidad que detenta el accionar del Ministerio de Justicia y Seguridad de la CABA en el acceso a los datos biométricos de personas que no se encuentran incluidas en la única base de datos sobre la cual funciona el Sistema de Reconocimiento Facial de Prófugos.

Sin embargo, la cuestión no encuentra frontera en simplemente divergencias cuantitativas. El mayor asombro encuentra lugar al repasar las personas incluidas en los listados que consignan los datos biométricos extraídos por el Gobierno local".

"[L]as personas consignadas resultan ajenas al sistema penal, no se encuentran prófugas, rebeldes o con un pedido de captura, o al menos hasta lo que se conoce.

Así, vale reiterar una vez más que en razón de la sensibilidad y protección legal que gozan los datos biométricos de las personas, el Ministerio de Justicia y Seguridad de la CABA sólo podría extraer tales datos siempre y cuando se trate de personas cuya búsqueda haya sido exigida por la justicia. Ello, de conformidad con lo establecido por el artículo 485 bis de la ley 5.688 y el Convenio de Cooperación Técnica celebrado entre el ReNaPer y el Ministerio de Justicia y Seguridad de la CABA. También podría suceder que deban ser necesarios tales datos en el marco de una investigación policial ´durante la etapa de prevención e investigación de delitos de acción pública´ (conforme cláusula segunda del Convenio citado). Es decir, el marco legal relativo a los datos biométricos es categórico al limitar su acceso a las circunstancias descriptas, por lo tanto, ´salvo orden judicial, se encuentra prohibido incorporar imágenes, datos biométricos y/o registros de personas que no se encuentran registradas en el CoNaRC´ (artículo 485 bis in fine).

[L]as personas que no se encuentran en la CoNaRC, están incluidas en el mismo listado que aquellas que sí. Es decir, los pedidos de datos personales de todo ese universo de personas se habrían realizado de idéntico modo y su tratamiento habría sido el mismo. En otras palabras, en un único listado se incluyen personas con órdenes de captura, prófugos o declarados en rebeldía y otras cuya razón se desconoce.

[R]esulta claro que tampoco podría esgrimirse que tal cuantiosa migración de datos biométricos obedece a consultas policiales efectuadas en operativos de seguridad o de siniestros en la vía público. Pues, tal posibilidad, carecería de asidero no sólo hasta el desmesurado número de extracciones, sino también en razón de las personas contenidas, conforme se ha exhibido a lo largo de la presente decisión".

# 1.3. JUZGADO DE 1° INSTANCIA EN LO CONTENCIOSO ADMINISTRATIVO Y TRIBUTARIO N° 4, SECRETARÍA N° 7. "OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.)". EXPEDIENTE N° 182908/2020. ACTUACIÓN N° 783420/2022. 7/9/2022.

**HECHOS**

El Gobierno de la Ciudad de Buenos Aires implementó el Sistema de Reconocimiento Facial de Prófugos (SRFP) en la jurisdicción de Ciudad Autónoma de Buenos Aires. El SRFP buscaba determinar si los rostros que se obtenían mediante el uso de cámaras de videovigilancia se encontraban y si correspondían o no con los rostros almacenados en la base de datos del sistema de Consulta Nacional de Rebeldía y Capturas (CoNaRC).

El Observatorio de Derecho Informático Argentino (O.D.I.A.) promovió una acción de amparo con el objetivo de que se declaren inconstitucionales la Resolución N° 398/MJYSGC/19 y la Ley N° 6339, en cuanto implementaron el SRFP, y también esta última en tanto modificó los artículos 478, 480, 484, 490 de la Ley N° 5688 e incorporó los artículos 480 bis y 490 bis. Ello, por considerar que afectaba, entre otros, el derecho a la libre circulación de las personas, el derecho de reunión, a la intimidad, a la no discriminación, a la igualdad y la protección de datos. O.D.I.A. explicó que los sistemas de reconocimiento facial funcionan mediante la comparación de características biométricas de dos rostros y que para poder llevar a cabo esa tarea deben aprender cuándo se trata de la misma persona y cuándo no. Eso lo logran a partir de una base de datos de distintas caras y mediante una carga de información constante que se logra analizando la totalidad de rostros que pasen por la cámara. En su presentación, destacó que, en otros lugares del mundo, previo a la aplicación de este tipo de sistemas, se habían llevado a cabo profundos debates por parte de la ciudadanía y las autoridades gubernamentales acerca de la posible afectación de datos personales y de si la implementación de cámaras de video vigilancia con sistemas de reconocimiento facial contribuía a mejorar la seguridad pública. Además, puso de resalto que en los lugares en los que se implementó el sistema se había establecido su justificación, legitimidad, necesidad y proporcionalidad mediante una Evaluación del Impacto en la Protección de Datos (EIPD) y que el Gobierno de la Ciudad de Buenos Aires no la había realizado, por lo que no era posible determinar el impacto y la posible afectación a los datos personales y otros derechos humanos básicos de los ciudadanos de la CABA. También sostuvo que el SRFP arrojaba casos de "falsos positivos" que generaban la detención errónea de personas que no tenían pedidos de captura, lo que daba como resultado que el sistema tenía un 50% de eficacia. Esa tasa de efectividad implicaba un prejuzgamiento de los habitantes de la Ciudad y una práctica discriminatoria contra las mujeres y minorías raciales. Además, destacaron que la base de datos de la CoNaRC, a partir de la cual el sistema buscaba personas, tenía errores. A este reclamo se adhirieron como actores dos personas y el Centro de Estudios Legales y Sociales (CELS) y se sumaron en condición de *amicus curiae* la Asociación Civil por la Igualdad y la Justicia (ACIJ), la Asociación Trabajadores del Estado (ATE), la Coordinadora contra la Represión Policial e Institucional (CORREPI), la Organización No Gubernamental "Derechos Digitales", la Organización Internacional de Derechos Humanos "Access Now", y la Fundación Vía Libre.

**DECISIÓN**

El Juzgado de 1° instancia en lo Contencioso Administrativo y Tributario N° 4 de CABA hizo lugar a la acción de amparo, declaró la inconstitucionalidad del artículo 1 de la Resolución Nº398/MJYSGC/19 ya que el Sistema de Reconocimiento Facial de Prófugos se implementó sin cumplir con los recaudos legales de protección de los derechos personalísimos de los habitantes de la Ciudad Autónoma de Buenos Aires, declaró la nulidad de lo actuado por el Ministerio de Justicia y Seguridad de la CABA en el marco del SRFP, y supeditó la puesta en funcionamiento de ese sistema a la constitución y funcionamiento de los órganos de control.

**ARGUMENTOS**

**1. Sistema de Reconocimiento Facial. Auditoría. Control de legalidad.**

"En resumen: a) la Defensoría del Pueblo se ve imposibilitada en su accionar como órgano de control, carácter atribuido mediante el art. 22 de la ley 1.845 de protección de datos personales y como auditora del SRFP en virtud del art. 3 de la resolución 398/2019 del Ministerio de Justicia y Seguridad de la CABA; b) la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia de la Legislatura no está constituida, pese a lo establecido en el art. 495 bis de la ley 5.688, por lo que el Poder Legislativo no está en condiciones de verificar el funcionamiento del SRFP; y c) tampoco el Ministerio de Justicia y Seguridad efectuó un control interno.

Y no es del caso, como parece se pretende por el GCBA que dichos controles legales puedan ser sustituidos por la auditoria del SRFP realizada por la Universidad de La Plata en el marco del Convenio acompañado en su contestación de demanda, lo cual, aclaro, no es óbice a que además se realice esa auditoria por la prestigiosa universidad. […] También cabe poner de relieve que dicho Convenio fue suscripto el 26/04/2021, es decir, aproximadamente dos años después de que el SRFP fue puesto en marcha y momento en el cual su funcionamiento se encontraba suspendido. En consecuencia, de ningún modo puede considerarse que las obligaciones legales relativas a la existencia de un organismo contralor y auditoría se encuentren cumplidas en virtud de un Convenio con la Universidad de La Plata. Por lo expuesto, cabe concluir que se puso en marcha el SRFP sin garantizar que éste cuente con los organismos de control que el cuerpo legal tanto nacional como internacional requieren, lo que se da de bruces con el principio de legalidad que debe regir todo accionar de la Administración".

**2. Sistema de Reconocimiento Facial. Cámara de seguridad. Auditoría. Usuarios y consumidores.**

"Otra cuestión a considerar son las fuentes de información del Sistema de Reconocimiento Facial de Prófugos. [E]l SRFP mediante las cámaras de video vigilancia capta imágenes que se visualizan y procesan en el Centro de Monitoreo Urbano (CMU) de la Policía de la Ciudad y las coteja con los datos biométricos contenidos en la CoNaRC, y en caso de advertir una coincidencia, emite una alerta para que personal policial actúe en consecuencia."

"De las consideraciones vertidas […] se desprende, por un lado, que no se encuentra inscripto el registro de datos relativo al sistema de videovigilancia en cumplimiento con lo dispuesto por los artículos 495 de la ley 5688 y 23 de la ley 1845. Por otro lado, el único registro sobre el cual opera el SRFP, es decir la CoNaRC, posee serias fallas que, en palabras del director [de la Dirección]

Nacional de Reincidencia, darían 'lugar a detenciones erróneas —falsos positivos— con las consecuencias disvaliosas que eso acarrearía al sujeto de derecho involucrado'. Estas falencias en el sistema conllevan a que personas que se encuentren dentro del territorio de la Ciudad sean confundidos con prófugos de la justicia y detenidos por las fuerzas de seguridad. Prueba de ello son los casos citados por el frente actor y los relatados por la Defensoría del Pueblo en su informe. Ahora bien, el hecho de que los errores y/o fallas recaigan sobre la base de datos de la CoNaRC y no sobre el Sistema de Reconocimiento Facial de Prófugos en sí mismo no puede ser considerado un argumento válido para soslayar los riesgos que entraña."

"El sistema debe ser comprendido de modo integral, en su totalidad y no en forma compartimentada. Más allá de que la CoNaRC no se encuentre dentro de la órbita del GCBA, lo cierto es que en virtud de los efectos que trae aparejado el uso de esta base en el marco del SRFP, deben desarrollarse mecanismos de articulación concretos para eliminar situaciones que vayan en detrimento de los derechos de las personas y ese es el sentido de los controles establecidos en el ámbito de la Ciudad pero que no se cumplen.

En efecto, los errores en la base de datos per se no generarían, en el marco de lo debatido en autos, una afectación de los derechos de las personas. Empero, en la utilización de aquélla por medio del SRFP se advierte lo contrario, y más aún ante la orfandad de controles legales, tales como la Defensoría del Pueblo de la Ciudad, la Comisión en la Legislatura, auditorías internas, etc. […] La mera eventualidad de estas falencias con las consecuencias que se derivan en los derechos personalísimos de las personas afectadas y la ausencia de controles —no por no estar contemplados en las leyes sino por la ausencia de debida implementación conforme a ellas—, demuestra un grave grado de riesgo de vulneración de derechos personales".

**3. Participación pública. Derechos humanos. Declaración de inconstitucionalidad. Defensor. Acceso a la justicia.**

"[S]e encuentra configurada una ilegítima restricción a los derechos constitucionales […]. [D]icha restricción es consecuencia de: a) la no constitución de la Comisión Especial en la Legislatura de la CABA; b) la falta de informes por parte de la Defensoría del Pueblo CABA; c) la inexistencia de un estudio de impacto sobre los derechos de los ciudadanos previa implementación del SRFP; d) de las fallas en las bases de datos de las que se nutre el SRFP; y e) la exclusión de la participación ciudadana. Es decir, no se centra en el SRFP en sí, sino en las consecuencias que acarreó su prematura implementación y su utilización en condiciones precarias de respeto por los derechos y garantías de las personas. De este modo, toda vez que el artículo 1 de la resolución 398/MJYSGC/19 implementó el Sistema de Reconocimiento Facial de Prófugos sin encontrarse cumplidos los mecanismos normativos necesarios para garantizar el adecuado uso del sistema —circunstancia que dio lugar a la afectación negativa de los derechos constitucionales referidos cuya protección no puede ser desconocida por la legislación ni por las autoridades locales— corresponderá declarar su inconstitucionalidad".

"[R]esulta necesario que al momento en que vuelva a ser implementado el SRFP: a) se cuente con los mecanismos de control de este sistema, es decir se constituya la Comisión Especial de Seguimiento de los Sistemas de Videovigilancia y que la Defensoría del Pueblo como órgano de contralor pueda ejercer eficazmente sus funciones; b) se constituya el registro de datos relativo

al sistema de videovigilancia; c) se realice un estudio previo relativo al impacto sobre los datos personales y d) se convoque a la ciudadanía a debatir las cuestiones relativas al Sistema de Reconocimiento Facial de Prófugos. Pues, lo contrario se traduce en graves consecuencias sobre los derechos de las personas que transitan la Ciudad […]".

**4. Datos biométricos. Registro Nacional de las Personas. Datos biométricos.**

"Una cuestión aparte surgida de las pruebas realizadas y de las que ha dejado constancia el Magistrado actuante de origen, está referido a la discordancia entre los registros de la CoNaRC y los datos biométricos que migraron desde ReNaPer hacia el Ministerio de Justicia y Seguridad de la CABA".

"[E]l listado remitido por el Ministerio de Justicia y Derechos Humanos de la Nación denota que las personas incluidas en la CONARC al 25/04/2019 eran aproximadamente 35.000 y al momento de la contestación del oficio ascendía a aproximadamente 40.000 registros (circunstancia que coincide con lo informado mediante nota no-2020-70688753-apnrnr#mj) mientras que, según lo informado por el RENAPER las solicitudes de datos biométricos efectuadas por el GCBA entre el 25/04/2019 y 20/12/2021 fueron 9.392.372 y entre el 21/12/2021 y el 09/03/2022 fueron 507.911. Esto es, un total de 9.900.282 extracciones en menos de dos años, dentro de los que el SRFP se habría encontrado mayormente inactivo".

"Esta verificación deja en evidencia un accionar jurídicamente reprochable del Ministerio de Justicia y Seguridad de la CABA en el acceso a los datos biométricos de personas que NO se encuentran incluidas en la única base de datos sobre la cual funciona el Sistema de Reconocimiento Facial de Prófugos, es decir, la CONARC, según surge del Informe del [ReNaPer ], y que únicamente a modo de ejemplo, se citan en el Anexo que forma parte de la presente resolución dado el volumen de información que ascienda a más de 15000 personas. Evidentemente, todas estas aseveraciones no se condicen con la información que surge del cuantioso listado aportado por el ReNaPer y su discordancia cuantitativa y cualitativa con el registro de la CoNaRC".

**5. Sistema de Reconocimiento Facial. Datos biométricos. Informe pericial.**

"El 11/04/2022 se ordenó, por el Magistrado de origen, en los términos del artículo 29 del Código CAyT, a la Policía de Seguridad Aeroportuaria llevar a cabo una pericia informática a fin de elaborar un informe que pormenorizadamente dé cuenta de los puntos que se repasan a continuación con su respectiva respuesta. Como se verá, cada uno de ellos confirma las irregularidades advertidas al momento de disponer la medida cautelar de autos".

"La pericia confirma que los datos biométricos de personas no requeridas judicialmente fueron utilizados para alimentar y posteriormente ser ejecutados por el SRFP. Asimismo, resalta que existen búsquedas respecto de personas sin que se haya identificado el juzgado que las habría solicitado. Cita como ejemplo de ello 84 casos que habrían sido ingresados en el SRFP a pedido de Interpol. Al respecto cabe recordar que dicho accionar se encuentra prohibido por el art. 485 *bis* en tanto dispone que el SRFP "será empleado únicamente para tareas requeridas por 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, datos biométricos y/o registros de personas que no se encuentren registradas en el CONARC".

"[…] Diferencia por un lado el borrado lógico, un procedimiento automático, típico y esperable para este tipo de sistemas, y por otro, el físico, procedimiento manual, voluntario y definitivo.

Así, la exhaustiva labor pericial verificó que 356 registros de personas cuyos datos biométricos fueron incorporados al motor de búsqueda del SRFP fueron eliminados voluntaria y manualmente (borrado físico definitivo). O sea que 356 personas fueron buscadas mediante el SRFP y la verificación de su motivo o justificación resulta imposible dado que sus registros fueron suprimidos de forma manual y voluntaria.

Obviamente, bajo los preceptos normativos repasados y el especial cuidado que merecen los datos personales, pareciera que lo atinado para el Sistema en estudio es que el borrado físico sea inexistente dado que, en estas condiciones da lugar a operaciones imposibles de ser rastreadas y/o analizadas posteriormente afectando la trazabilidad de lo hecho".

"Como corolario del presente informe, los consultores técnicos (veedores) y perito interviniente, concluyen que resulta de prístina claridad que el SRPF posee inconsistencias y errores en los procesos administrativos de alta/baja/modificación, observando también vestigios del entorno de desarrollo que deberían encontrarse solucionados al momento de implementarse en modelo de producción' (el destacado me pertenece)".

## 1.4. CÁMARA DE APELACIONES EN LO CONTENCIOSO ADMINISTRATIVO, TRIBUTARIO Y DE RELACIONES DE CONSUMO. SALA I. SECRETARÍA ÚNICA. "OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.)". EXPEDIENTE N° 182908/2020. ACTUACIÓN N° 1055665/2023. 28/4/2023.

**HECHOS**

El Gobierno de la Ciudad de Buenos Aires implementó el Sistema de Reconocimiento Facial de Prófugos (SRFP) en la jurisdicción de Ciudad Autónoma de Buenos Aires. El SRFP buscaba determinar si los rostros que se obtenían mediante el uso de cámaras de videovigilancia se encontraban y si correspondían o no con los rostros almacenados en la base de datos del sistema de Consulta Nacional de Rebeldía y Capturas (CoNaRC).

En razón de ello, el Observatorio de Derecho Informático Argentino (O.D.I.A.) promovió una acción de amparo con el objetivo de que se declaren inconstitucionales la Resolución N° 398/MJYSGC/19 y la Ley N° 6339, en cuanto implementaron el SRFP, y también esta última en tanto modificó los artículos 478, 480, 484, 490 de la Ley N° 5688 e incorporó los artículos 480 bis y 490 bis. Ello, por considerar que afectaba, entre otros, el derecho a la libre circulación de las personas, el derecho de reunión, a la intimidad, a la no discriminación, a la igualdad y la protección de datos.

El juzgado de primera instancia en lo Contencioso Administrativo y Tributario N° 4 dictó sentencia contra el GCBA y suspendió el uso del SRFP. En la sentencia el juzgado de grado mencionó que aquello no significaba una merma de los restantes sistemas de videovigilancia (monitoreo urbano), preventivo y forense; ni mucho menos un menoscabo en el servicio de seguridad pública, dado que el SRFP se encontraba inactivo por decisión del GCBA. Además, sostuvo que el problema no se centró en el SRFP en sí mismo, sino en las consecuencias que acarreaba su prematura implementación y su utilización en condiciones precarias de respeto por los derechos y garantías de las personas. Por ello, explicó que para que volviera a ser implementado, debían funcionar los mecanismos de control, constituirse un registro de datos relativo al sistema de videovigilancia, realizarse el estudio previo de impacto sobre los datos personales (Evaluación del Impacto en la Privacidad —EIP—) y convocarse a la ciudadanía a debatir sobre dicho mecanismo.

Contra esa decisión, O.D.I.A. junto al CELS y dos personas que se presentaron como actores, interpusieron un recurso de apelación. La parte actora criticó el fallo de primera instancia por mantener la vigencia del SRFP supeditada al funcionamiento de los órganos de control (Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia y Defensoría del Pueblo local) pues según el peritaje técnico el sistema era deficiente y no resultaba suficiente la existencia de mayores controles y reaseguros para evitar la vulneración de los derechos de las personas. Además, destacó que eran las características del sistema lo que lo tornaba inseguro, más allá de los contralores que pudieran desarrollar los organismos competentes, por lo que no existía ningún mecanismo de vigilancia que hiciera compatible esta herramienta con los derechos personales afectados. Asimismo, cuestionó la falta de participación y debate ciudadano antes de la sanción de las normas que regulan el SRFP. Por otro lado, afirmó que el SRFP violaba los derechos personales a la intimidad, privacidad y de protección de datos personales porque las

cámaras captaban la totalidad de los rostros que pasaban por delante de ella y porque dotaba al Estado de información precisa respecto de los lugares públicos dentro de la Ciudad Autónoma de Buenos Aires donde se encontraban las personas. En esa línea, criticó que en la sentencia de primera instancia no se había analizado concretamente la afectación que el SRFP provocaba sobre tales derechos y que el SRFP realizaba un tratamiento de datos personales sensibles que requería el consentimiento del titular de la imagen. Por su parte, el CELS, entre otras cosas, sostuvo que el software que utilizaba el SRFP era discriminatorio y, por ende, atentaba contra el derecho a la igualdad toda vez que la precisión de los sistemas de reconocimiento facial variaba en función del color, la raza, el género de las personas, incrementando las posibilidades de errores y de falsos positivos, generando impactos desproporcionados sobre grupos en situación de vulnerabilidad, entre las cuales se encontraban las mujeres.

**DECISIÓN**

La Sala I de la Cámara de Apelaciones en lo Contencioso Administrativo, Tributario y de Relaciones de Consumo, no hizo lugar al recurso de apelación interpuesto por O.D.I.A, ni por los demás actores. Sin embargo, sí hizo lugar parcialmente a los agravios del CELS y, en consecuencia, ordenó que la rehabilitación del funcionamiento del SRFP, además de quedar supeditada a la constitución y debido funcionamiento de los órganos de control, quedará sujeta a la realización de las investigaciones y pruebas necesarias sobre el software que utiliza el SRFP. Asimismo, requirió que antes de poner en funcionamiento el SRFP, se publicite e informe 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 entienden necesarias; escrutinios que deberán ser transmitidos a la autoridad de aplicación del SRFP, con el propósito de que exponga las explicaciones necesarias y, de entenderlo procedente, adopte medidas que perfeccionen el sistema.

**ARGUMENTOS**

1. **Derecho a la privacidad. Derecho a la intimidad. Derecho a la vida privada y familiar. Espacio público.**

"[L]a declaración de inconstitucionalidad dispuesta por la *a quo* no refiere al sistema en sí mismo sino a su puesta en funcionamiento. Por eso, el resolutorio decide a continuación supeditar la ejecución del SRFP a la constitución y debido funcionamiento de los órganos de control (Comisión Especial de seguimiento de los sistemas de video vigilancia y Defensoría del Pueblo de la Ciudad). Así las cosas, más allá de los términos utilizados por la jueza de grado, en la especie no se ha declarado la inconstitucionalidad del dispositivo, sino que se ha considerado ilegítimo el uso (obrar) que las autoridades hicieron de él. [...] En síntesis, en autos, el fallo impugnado no admitió, en concreto, la inconstitucional de una norma, sino que reconoció la configuración de un obrar ilegítimo de las autoridades"

"[E]n el presente caso, la parte actora cuestiona una herramienta [Sistema de Reconocimiento Facial de Prófugos —SRPF—] prevista normativamente para el cumplimiento de una función esencial del Estado: la seguridad pública.

La tensión, entonces, se manifiesta entre —por un lado— el dispositivo que el accionado utiliza para satisfacer ese deber irrenunciable del Gobierno; y, por el otro, los derechos que la parte actora identifica como vulnerados con motivo de la utilización del SRFP (no discriminación, privacidad, intimidad, presunción de inocencia, libertad ambulatoria, y protección de datos personales)".

"[E]l sistema fue impugnado por la parte actora con sustento en que vulnera (entre otros) los derechos a la privacidad e intimidad, así como a la protección de los datos personales, es dable recordar que estos se insertan dentro del respeto a la vida privada que tiene regulación en el plexo constitucional (artículo 19, [Constitución Nacional] y 12, [Constitución de la Ciudad Autónoma de Buenos Aires]). Sobre estas bases, cabe recordar que las acciones privadas quedan exentan de la autoridad de los magistrados siempre que no ofendan el orden y la moral pública, y tampoco perjudiquen a terceros.

Es necesario aclarar que existe diferencia entre intimidad y privacidad: ´[l]a intimidad sería la esfera persona que está exenta del conocimiento generalizado de terceros, y la privacidad sería la posibilidad irrestricta de realizar acciones privadas (que no dañan a otros) por más que se cumplan a la vista de los demás y que sean conocidas por estos´; aunque ambos derechos forman parte de la ´[...] zona de reserva personal, propia de la autonomía del ser humano´ (conforme Bidart Campos, Germán J., Manual de la Constitución Reformada, T.I., Ediar, Buenos Aires, 2013, página 522).

No obstante, lo señalado, dichos conceptos se utilizan habitualmente como sinónimos".

"[E]n términos generales, se coincide con la parte demandante en que la vida privada y la intimidad personal (a las cuales se vincula claramente la protección de los datos personales —entre ellos, la imagen—) abarca más que la vida doméstica dentro del hogar y se extiende a la vida de las personas en el espacio público".

**2. Reglamentación. Razonabilidad. Principio de proporcionalidad.**

"[D]efinidos los derechos en tensión y las causales que habilitan su reglamentación, es preciso realizar un balance entre el interés de las personas a no sufrir una invasión a su privacidad y el interés estatal en el cumplimiento del deber de garantizar la seguridad pública. A ese fin es necesario ponderar si la medida adoptada para alcanzar la finalidad perseguida supera los filtros de necesidad, adecuación y proporcionalidad (conforme doctrina que emana de la [Corte Suprema de Justicia de la Nación], in re "Gualtieri Rugnone de Prieto Emma Elidia y otros s/ Sustracción de menores de 10 años —Causa N° 46/85 A—", G. 1015. XXXVIII. RHE, sentencia del 11 de agosto de 2009, Fallos: 332:1835, disidencia del juez Juan Carlos Maqueda)".

"[L]a materia que nos ocupa se vincula con la potestad del Estado de regular los derechos. Cabe recordar que el Estado no solo garantiza los derechos mediante abstenciones sino también a través de acciones positivas. Más aún, "[...] el Estado puede regular cualquier derecho y [...] su mayor o menor densidad depende las circunstancias sociales, políticas o económicas, sin perjuicio de que el Estado siempre deba respetar el núcleo de estos (sustantividad)" (Balbín, Carlos F.,

Tratado de Derecho Administrativo, 2da. Edición actualizada y ampliada, T.II, Editorial La Ley, Buenos Aires, 2015, pág. 642)".

"Si bien en algunos supuestos, el alcance del poder estatal de regulación ha sido establecido por el convencional con sustento en la necesidad (dentro de una sociedad democrática) de resguardar la seguridad, el orden, la salud y la moral públicas, o los derechos y libertades de terceros; en todos los casos, la restricción (regulación) siempre debe satisfacer el principio de razonabilidad (abarcativo del principio de proporcionalidad) en términos constitucionales. Como señala la doctrina, ´[...] definido el campo estatal de regulación de los derechos (restricciones), y particularmente sus límites, el Estado puede en este contexto jurídico recortar más o menos, según su discrecionalidad´, sin obviamente alterarlos. No obstante, la restricción depende de las características del derecho a limitar y del derecho que se pretende proteger con esa limitación; pues se recortan derechos para satisfacer otros derechos. En otros términos, ´[...] las restricciones son válidas siempre que el Estado persiga un interés legítimo y razonable (interés colectivo), esto es, [...] el reconocimiento de otros derechos con intervención del Legislador´ (conforme Balbín, Carlos F., Tratado de Derecho Administrativo, 2da. edición actualizada y ampliada, T.II, Editorial La Ley, Buenos Aires, 2015, T. II, pág. 417 y ss.)".

"[E]l principio de proporcionalidad (que integra el de razonabilidad) se conforme de tres subprincipios, a saber: adecuación, necesidad, y proporcionalidad en sentido estricto. El primero de los mencionados (adecuación) evalúa dos cuestiones: por un lado, la finalidad que persigue la norma; y, por el otro, si esta se halla incluida dentro de los fines constitucionales (es decir, fin lícito e idoneidad para alcanzarlo). El segundo (necesidad) obliga a ponderar si la restricción dispuesta sobre el derecho es la menos gravosa entre otras igualmente posibles en el mismo grado de eficacia. Finalmente, el último subprincipio (proporcionalidad propiamente dicha) exige sopesar los perjuicios que la limitación del derecho ocasiona a su titular y las ventajas que se obtienen con motivo de su aplicación; ello, con el objetivo de determinar si el grado de afectación se encuentra justificado (es decir, cuál de los derechos en tensión debe privilegiarse). Es preciso agregar —a su respecto— que, en términos generales, su aplicación forma parte del control de la actividad administrativa sobre los derechos".

"No puede perderse de vista que la reforma constitucional de 1994 dio preeminencia al control de la actividad estatal a través de diversos organismos cuyo objetivo es garantizar una mayor transparencia, eficacia e idoneidad de la gestión de Gobierno.

Transparencia y control son herramientas ineludibles para lograr la confianza social en torno a que las decisiones estatales respetan el principio de legitimidad y que, de corroborarse lo contrario, los poderes del Estado —en sus respectivos ámbitos de actuación— intervendrán para revertir cualquier tipo de ilegalidad e irrazonabilidad, sancionando a los responsables mediante los mecanismos jurídicos existentes.

[E]l SRFP constituido ha sido atado a una serie de controles tendientes a garantizar su funcionamiento acorde a las normas constitucionales que protegen los derechos personales de los individuos que transitan por la Ciudad. El régimen normativo lo somete a contralores específicos: la actuación de la Comisión prevista en el artículo 490 bis de la Ley N° 5.688; la creación del registro ordenado en el artículo 490 de ese mismo cuerpo legal; y el establecido en

la Resolución N° 398/2019 —DP [Defensoría del Pueblo]—. También lo sujetó a los controles previstos en normas generales: la Ley N° 1.845 —nuevamente, la intervención del Defensor del Pueblo—; y la Ley N° 70 (al imponer un control interno de los órganos que conforman la administración centralizada, entre otros posibles).

En este contexto de diversidad de mecanismos de control —cuya implementación no se ha producido aun de modo cabal; o cuya intervención ha sido tardía o se ha visto demorada por circunstancias imponderables (pandemia) o por omisiones de las autoridades competentes—, su falta de actuación trasunta un incumplimiento de los preceptos jurídicos y, consecuentemente, una vulneración del principio de legalidad.

No obstante, lo señalado, no es posible afirmar (con la certeza que exige la declaración de inconstitucionalidad de las normas) que el funcionamiento del SRFP no resulte eficiente si este estuviera sometido a todas las fiscalizaciones que las normas especiales y generales prevén. El desconocimiento actual de los resultados que el aludido contralor podría provocar sobre el sistema impide su anulación como herramienta idónea en el cumplimiento de los objetivos para los cuales fue constituida.

El eventual uso ilegítimo que las autoridades competentes pudieran haber hecho de este mecanismo (cuestión que ha sido motivo de una denuncia penal a cargo de otro fuero y cuyo resultado se desconoce) no justifica su inoperancia para alcanzar los fines que le dieron origen y, por ende, no permite ese solo hecho la anulación de su uso".

"[N]o puede suponerse de ante mano la ineficacia de las tareas de control que, cabe aclarar, debieran abarcar la totalidad del sistema (incluido el algoritmo de identificación de los datos biométricos y la base de datos de la CONARC, mencionados por el apelante). Ello así, toda vez que es razonable presumir que la actuación de los organismos de control (al que el decisorio de grado somete la reactivación del SRFP) podrá dar lugar a eventuales objeciones que permitirán adoptar las medidas necesarias para subvertir el porcentaje de detenciones indebidas que el apelante denuncia (140 sobre 1600 aprensiones).

Lo expuesto es, obviamente, sin perjuicio de que si los organismos encargados de verificar el funcionamiento adecuado de la herramienta, tras haber ejercido sus competencias, admitieran que aquella vulnera derechos constitucionales o que padece de defectos que la tornan inconciliable con el bloque de convencionalidad, los actores planteen nuevamente la ilegitimidad del SRFP mediante los carriles procesales que consideren más adecuados sobre la base de esas nuevas circunstancias fácticas".

"En síntesis, la parte actora no logró demostrar que el cabal ejercicio de los contralores normativamente impuestos sobre el SRFP no resultará eficaz para resguardar los derechos personales cuya vulneración sustenta en el uso de este Dispositivo".

### 3. Protección de datos personales. Consentimiento.

"[L]a parte actora no peticionó la declaración de inconstitucionalidad de las excepciones a la necesidad de dar consentimiento que la Ley N° 1.845 establece. Además, la mención que dicha parte efectuó con relación a la ausencia de un análisis sobre la tensión que se generaba entre el

consentimiento que los regímenes protectorios para el tratamiento de datos personales de carácter sensible y las correspondientes excepciones que obran en el artículo 7, inciso 4 de la Ley N° 1.845 (CABA) y en el artículo 5, inciso 2, apartado "b" de la Ley N° 25.326 no contienen un desarrollo suficiente y adecuado que justifique declarar inconstitucional las excepciones al consentimiento en virtud de los fines sobre los que se asienta".

**4. Libertad de tránsito. Principio de inocencia. Protección de datos personales. Derecho a la privacidad. Detención de personas. Control de legalidad.**

"Los accionantes también invocaron la vulneración de los derechos a la libertad ambulatoria y la presunción de inocencia. Estos encuentran sustento en el artículo 18 de la Constitución Nacional en cuanto garantiza que nadie puede ser condenado sin juicio previo.

Sin perjuicio de la alta estima que estos derechos poseen, lo cierto es que caben a su respecto idénticas apreciaciones a las realizadas respecto de los derechos a la privacidad y a la protección de datos personales.

Su afectación —con motivo de la utilización del SRFP [Sistema de Reconocimiento Facial de Prófugos]— no puede ser ponderada en la actualidad con estándares de certeza debido a la falta de intervención (oportuna y por el momento) de los mecanismos de control y transparencia que el plexo normativo previó para fiscalizar los beneficios o deficiencias que dicha herramienta apareja.

Nótese que, en términos hipotéticos, el correcto funcionamiento del mecanismo que nos ocupa debiera evitar la generación de falsos positivos. Esa circunstancia evitaría —por un lado— detenciones y demoras indebidas que transgredan el principio de inocencia; y, por el otro, la configuración de restricciones ilegítimas a la libertad ambulatoria".

**5. Sistema de Reconocimiento Facial. Declaración de inconstitucionalidad. Control judicial.**

"[L]a constitucionalidad de las normas que crearon e implementaron el SRFP no puede ser determinada a partir de su uso prematuro por parte de la autoridad de aplicación. Es decir, cuando: 1) aún no se hallaban vigentes o no estaban en condiciones de funcionar los controles que el mismo ordenamiento impugnado impuso y los previstos en otros plexos jurídicos vinculados a la materia objeto de debate; 2) todavía no se habían acatado otras imposiciones registrales que hacían a su funcionamiento transparente; y 3) no se habían adoptado las medidas de control interno que demostraran la regularidad de las bases de datos sobre las que el mecanismo fue apoyado a fin de evitar irregularidades que afectasen los derechos de quienes transitaran por la ciudad".

"[L]a ausencia de los controles específicamente establecidos por diversos plexos normativos (cuya finalidad —entre otras— es custodiar el uso regular del sistema; objetar y evidenciar las posibles irregularidades; y ponderar su efectivo funcionamiento —entendido como la posibilidad de observar si la aplicación cotidiana del SRFP, con el objeto de garantizar la seguridad pública, produce o no una vulneración inadecuada, innecesaria o desproporcionada de los derechos personales en juego—) impide arribar a la conclusión pretendida por el aquí recurrente. En otras palabras, conforme el análisis realizado, resulta precoz la declaración de inconstitucionalidad de

la Ley N° 6.339, circunstancia que conduce a rechazar el agravio de la parte actora referido a la falta de proporcionalidad de la medida impugnada (SRFP)".

**6. Igualdad. Vulnerabilidad. Auditoría. Sistema informático. Sistema de Reconocimiento Facial.**

"[E]s dable observar […] que cierta información respecto del funcionamiento técnico del sistema no fue develada en esta causa. Se desconoce entonces si —como adujo el recurrente— es cierto que el mecanismo no responde de igual manera frente a determinadas características personales (género, raza, color)".

"[E]l régimen legal *in totum* regulatorio del funcionamiento del SRFP previó múltiples controles a cargo de diferentes autoridades. Es decir, se impuso un mayor contralor en virtud de la trascendencia de los derechos sobre los que dicha herramienta opera (v. gr. privacidad, intimidad, protección de datos). En ese contexto, la certificación de si el mecanismo impugnado produce o no una vulneración del principio de igualdad (en otras palabras, si brinda respuestas discriminatorias basadas en categorías sospechosas o no) resulta esencial para determinar si el SRFP resulta constitucional o inconstitucional. Por ello, corresponde ordenar que la rehabilitación del funcionamiento del SRFP, además de quedar supeditada a la constitución y debido funcionamiento de los órganos de control (tal como dispuso la sentencia de grado; actuación N° 2453371/2022), también queda sujeto a la realización de las investigaciones y pruebas necesarias sobre el software que utiliza el SRFP (por parte de los organismos de control con asistencia del accionado o de quien este considere adecuado), para determinar si su empleo tiene un impacto diferenciado según las características personales de los individuos afectados".

**7. Sistema de Reconocimiento Facial. Participación pública. Ciudad Autónoma de Buenos Aires. Publicidad. Democracia.**

"[Se] cuestionó la falta de participación y debate ciudadano antes de la sanción de las normas en las que se sustenta el SPF [Sistema de Reconocimiento Facial de Prófugos].

[L]a participación se vincula a las formas semidirectas de democracia y que esa intervención en el proceso de formulación de las decisiones políticas, jurídicas y administrativas del gobierno obliga a reconocer a toda persona el derecho a tomar parte directamente en el gobierno de su país a través de cualquier mecanismo de participación popular (CSJN, "Aníbal Roque Baeza c/ Nación Argentina. Founrouge, Alberto M.", sentencia del 28 de agosto de 1984, Fallos 306:1125); v. gr. el FOSEP.

[L]a transcendencia del derecho de participación en los asuntos públicos que dio lugar a la creación legal de los FOSEP [Foros de Seguridad Pública], impone adoptar una decisión que garantice el ejercicio de este derecho por parte de los vecinos de la Ciudad.

Si bien se advierte que la parte actora no acreditó la existencia de demandas o propuestas de organizaciones o vecinos respecto del SPF en los FOSEP o de su falta de tratamiento en esas sedes, el demandado tampoco demostró haber dado a publicidad la medida en forma previa a su establecimiento ni haber realizado alguna convocatoria a la comunidad con relación a la materia debatida.

Así las cosas, toda vez que estos espacios (conforme artículo 22) ´[...] promueven la efectiva participación ciudadana para la formulación de propuestas y seguimiento en materia de políticas públicas de seguridad', corresponde ordenar que —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 (a través de los mecanismos habituales) la existencia de esta herramienta, su funcionamiento y las reglas jurídicas que en su totalidad lo rigen. Ello, para un cabal conocimiento de la misma y con el objetivo de que aquellos puedan ejercer el control ciudadano que la Ley N° 5.688 habilita, vertiendo 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".

# 2. JURISPRUDENCIA INTERNACIONAL

## 2.1. CORTE SUPREMA DE JUSTICIA DE JAMAICA. "ROBINSON V. FISCAL GENERAL". CASO N° 2018HCV01788. 12/04/2019.

**HECHOS**

Un ciudadano de Jamaica, diputado y secretario general del Partido Nacional del Pueblo impugnó la constitucionalidad de la Ley Nacional de Identificación y Registro (National Identification and Registration Act —NIRA—, por su sigla en inglés) sancionada por el parlamento de ese país. El ciudadano consideraba que algunas de las disposiciones de la ley violaban el derecho a la igualdad, la libertad, la seguridad y la intimidad. La ley —que aún no había entrado en vigor— buscaba proporcionar un sistema de recopilación de datos de todos los ciudadanos de Jamaica y de aquellos que vivieran en el país durante al menos seis meses de un año calendario. Para tal fin, requería que las personas solicitaran el registro y en caso de no hacerlo quedaban expuestas al riesgo de una sanción penal. El sistema utilizado por la ley proponía recopilar, entre otras cosas, los datos biométricos, la información demográfica y los números de referencia nacional, como el número de contribuyente y la licencia de conducir, con el objetivo de crear una base de datos nacional de identificación civil que se almacenaría indefinidamente en los sistemas gubernamentales. Al momento de registrarse, a las personas se les asignaría un número de identificación nacional (*National Identification Number* —NIN—), lo que las haría elegibles para la entrega de una tarjeta de identificación nacional (*National Identification Card* —NIC—). El NIN o la NIC era imprescindibles para acceder a bienes o servicios prestados por las autoridades. Sin embargo, el sistema también permitía el acceso de terceros a los datos personales sin suficientes garantías de protección.

**DECISIÓN**

La Corte Suprema de Justicia de Jamaica decidió que la Ley Nacional de Identificación y Registro, en su totalidad, era inconstitucional, nula y sin valor porque violaba el derecho a la intimidad y la igualdad.

**ARGUMENTOS**

**1. Libertad. Derecho a la intimidad. Principio de dignidad humana.**

"El tema subyacente de esta reivindicación es la libertad y la intimidad. Dos importantes tribunales finales se han pronunciado sobre estas cuestiones. En el Tribunal Supremo canadiense, Dickson J (como era en aquel momento) en Big M Drug Mart Ltd 18 DLR (4th) 321 dijo lo siguiente sobre la libertad, en el contexto de la libertad religiosa, en la página 354:

> 95. La libertad puede caracterizarse principalmente por la ausencia de coacción o coerción. Si una persona se ve obligada por el Estado o por la voluntad de otra a seguir un curso de acción o de inacción que de otro modo no habría elegido, no está actuando por propia voluntad y no puede decirse que sea verdaderamente libre. Uno de los principales objetivos de la Carta es proteger dentro de la razón de la coacción o la restricción. La

> coacción no sólo incluye formas tan flagrantes de coacción como las órdenes directas de actuar o abstenerse de actuar so pena de sanción, la coacción incluye formas indirectas de control que determinan o limitan cursos alternativos de conducta disponibles para otros. La libertad en sentido amplio abarca tanto la ausencia de coacción y coerción como el derecho a manifestar creencias y prácticas. La libertad significa que, sin perjuicio de las limitaciones necesarias para proteger la seguridad, el orden, la salud o la moral públicos, o los derechos y libertades fundamentales de los demás, nadie debe ser obligado a actuar de manera contraria a sus creencias o a su conciencia".

"Este pasaje es de aplicación general y puede servir de base para entender la libertad. [L]a cita explica en qué consiste un aspecto de la Carta de Jamaica. Los derechos relativos a las libertades de pensamiento, religión, reunión pacífica, circulación y no discriminación se refieren a la libertad de no ser obligado a hacer o dejar de hacer algo que uno no quiere hacer cuando no hay ninguna razón de peso, salvo la opinión de otra persona, incluidos el ejecutivo y el legislativo, para que uno lo haga".

"[L]a intimidad, tal como se entiende ahora, tiene al menos tres aspectos: intimidad de la persona, intimidad informativa e intimidad de elección. Estos aspectos de la intimidad no surgen porque los confiera el Estado, sino que los poseen todas las personas por el mero hecho de ser humanas".

"[Esto] no debe considerarse nuevo o extraño. De hecho, la nueva Carta de Jamaica se basa en la dignidad inherente de los seres humanos. El artículo 13 (1) (a) es un preámbulo que establece que el ´Estado tiene la obligación de promover el respeto universal y la observancia de los derechos humanos y las libertades´ y además que todos los jamaiquinos tienen derecho a estos derechos ´en virtud de su dignidad inherente como personas y como ciudadanos de una sociedad libre y democrática´ ((énfasis añadido) (sección 13 (1) (b)). Por tanto, los derechos y libertades garantizados están concebidos para hacer efectiva y reforzar la dignidad inherente a las personas. Dignidad, en su esencia, significa digno de respeto y honor. Inherente significa algo que está, en este caso en las personas, como una característica o atributo permanente y esencial. Nuestro legislador ha dicho que todos los jamaiquinos, por el mero hecho de ser ciudadanos de Jamaica, tienen un atributo permanente y esencial de honor y respeto. A esto se añade su condición declarada de ciudadanos de una sociedad libre y democrática".

"[E]xiste jurisprudencia que indica que el derecho a la intimidad es polifacético. La intimidad implica (a) la integridad corporal, mental y emocional; (b) el anonimato; y (c) la protección de la información personal. La intimidad en una sociedad libre y democrática reconoce que el individuo tiene el control sobre si su información biográfica y/o demográfica se comparte y en qué circunstancias se comparte. La intimidad en una sociedad libre y democrática reconoce que la información biométrica de una persona es suya y que ésta conserva el control sobre dicha información en virtud de su dignidad inherente como ser libre y autónomo. Por lo tanto, la toma obligatoria de cualquier dato biométrico es una violación del derecho a la intimidad: intimidad de la persona, intimidad informativa. El carácter obligatorio de la NIRA sugiere claramente que se ha eliminado la intimidad de elección. La única cuestión que queda por dilucidar es si existe justificación en el sentido de la Carta de Jamaica o si la violación entra dentro de las secciones de la Carta que están exentas de los derechos y libertades que prevé. Incluso en los espacios públicos no se pierde toda la intimidad. El público no espera que su información biométrica sea tomada

por nadie y utilizada de manera no autorizada por él. Así pues, en términos generales, no se puede eludir el derecho a la intimidad utilizando métodos no intrusivos, como el software de reconocimiento facial y otras aplicaciones para recoger información biométrica y utilizarla sin permiso de la persona".

"En algunos contextos se ha dicho que los ciudadanos honrados no tienen nada que temer. Sin embargo, eso es malinterpretar el derecho a la intimidad en una sociedad libre y democrática. Las sociedades libres y democráticas aceptan y actúan sobre la premisa de que el individuo tiene derecho a que le dejen en paz, a ser anónimo en la medida de lo posible y a conservar el control sobre su hogar, su cuerpo, su mente, su corazón y su alma. Esto forma parte de la dignidad inherente al ser humano".

**2. Prueba. Carga de la prueba. Razonabilidad. Reglamentación de los derechos.**

"[E]l Parlamento no debe aprobar ninguna ley que viole el derecho o derechos del ciudadano, y si el ciudadano ha demostrado que sus derechos han sido violados, entonces debe ser necesariamente el infractor quien justifique su violación. El examen consiste en analizar si la violación está justificada de forma demostrable. Los antiguos casos de la Carta de Derechos, aunque útiles, nunca tuvieron este entendimiento y quizás no pudieron porque no existía una disposición como la sección 13 (2) en la anterior Carta de Derechos. Por lo tanto, adopto plena y completamente el test establecido por Dickson CJ en [R v Oakes (1986), resuelto por el Tribunal Supremo canadiense]".

"[E]n virtud de la Carta de Jamaica, no corresponde al demandante, como en los casos Marpin, Wormes y Madhewoo, demostrar una negativa, a saber, que la ley no estaba razonablemente justificada en una sociedad libre y democrática; corresponde al infractor demostrar que la ley es justificable en una sociedad libre y democrática. Se trata de un cambio radical y fundamental que debe reconocerse. Todo lo que tiene que hacer el demandante es demostrar, bien mediante un análisis textual, bien mediante pruebas, o ambas cosas, que se ha producido, se está produciendo o es probable que se produzca una violación. Si el caso no entra dentro de los supuestos enumerados en el apartado 2 del artículo 13 de la Carta de Jamaica, el único puerto seguro que le queda al infractor es demostrar que la ley es justificable en una sociedad libre y democrática".

"[S]i el demandante establece un caso prima facie y el Estado responde y las cosas están equilibradas, entonces el demandante debe tener éxito porque un caso prima facie de violación sólo puede superarse con pruebas claras de que la violación estaba justificada. Si el Estado no puede demostrar una justificación convincente, no podrá desestimar la demanda porque los litigios constitucionales son sui generis en el sentido de que la ley presume que el demandante tiene la intención de disfrutar plenamente del derecho cuya violación se alega, a menos que exista una justificación clara de su restricción. Un caso equilibrado tras una demostración prima facie debe significar que el Estado no ha justificado claramente la restricción del derecho y, por tanto, el demandante debe seguir disfrutando del derecho en toda su extensión".

**3. Razonabilidad. Principio de proporcionalidad. Control de constitucionalidad. Democracia.**

"Este examen de proporcionalidad ha sido descrito por el Dr. Dhananjaya Chandrachud J. en Justice K Puttaswamy (Retd.) and Anr. v. Union of India Writ Petition (Civil) NO 494 de 2012 (pronunciada el 26 de septiembre de 2018). [El magistrado] dijo en los párrafos 197—198:

> El examen de proporcionalidad, que comenzó como un conjunto no escrito de principios generales del derecho, constituye hoy en día la norma judicial dominante de ´mejores prácticas´ para resolver litigios que impliquen un conflicto entre las pretensiones de dos derechos o entre un derecho y un interés gubernamental legítimo. Se ha convertido en una ´pieza central de la jurisprudencia´ en todo el continente europeo, así como en jurisdicciones de derecho común como el Reino Unido, Sudáfrica e Israel […]. Se ha elevado al rango de principio constitucional fundamental y representa un cambio global de una cultura de autoridad a una cultura de justificación […]
>
> **[…] El examen de proporcionalidad estipula que la naturaleza y el alcance de la injerencia del Estado en el ejercicio del derecho …deben ser proporcionales al objetivo que se pretende alcanzar […]".** (énfasis añadido a la sentencia)

"[E]n una democracia constitucional en la que hay constitucionalismo y no sólo la existencia de una Constitución, el ejercicio del poder ya sea ejecutivo, legislativo o judicial, ya no se basa simplemente en la idea de tener el poder de hacer lo que se está autorizado a hacer, sino que también va acompañado de la justificación de las decisiones y acciones. Por eso los jueces motivan sus decisiones. Ahora, en el contexto de los recursos de inconstitucionalidad, la justificación se exige a los poderes ejecutivo y legislativo. En una palabra, la proporcionalidad tiene que ver con la responsabilidad".

"[E]l asunto canadiense R v Oakes 26 DLR (4th) 200 respalda esta postura [aplicar un examen de proporcionalidad]. En dicho asunto se aplicó el criterio de proporcionalidad a la legislación canadiense. Ello requiere un examen detenido […]".

"Aunque [el juez] Dickson CJ [en la sentencia R v Oakes 26 DLR (4th) 200] enumeró tres criterios que deben cumplirse para superar el requisito de proporcionalidad, si se incluye el criterio de la finalidad adecuada, son cuatro. [En ese caso] previó una prueba de dos etapas en la que la primera etapa consiste en decidir si la ley cumplía el criterio de la finalidad adecuada, es decir, un objetivo que fuera tan importante (no trivial) que fuera necesario violar el derecho fundamental. Está claro que […] si no se cumplía el criterio de la finalidad adecuada, la ley era necesariamente inconstitucional y no había necesidad de pasar a considerar los otros tres criterios, que juntos constituyen la segunda fase. Por lo tanto, no importa si se trata de un examen en dos fases o de un examen con cuatro partes, porque al final se aplican los cuatro criterios. Desde mi punto de vista, prefiero pensar en el examen como cuatro criterios y no en dos etapas. Los cuatro criterios son: b) la ley debe estar dirigida a un fin adecuado que sea lo suficientemente importante como para justificar la restricción de los derechos o libertades fundamentales; c) las medidas adoptadas deben estar cuidadosamente diseñadas para alcanzar el objetivo en cuestión, es decir, racionalmente relacionadas con el objetivo, lo que significa que las medidas son capaces de alcanzar el objetivo. Si no lo son, son arbitrarias, injustas o se basan en consideraciones irracionales; d) los medios utilizados para alcanzar el objetivo deben violar el derecho lo menos posible; e) debe existir proporcionalidad entre los efectos de las medidas que limitan el derecho

y el objetivo que se ha identificado como suficientemente importante, es decir, el beneficio derivado de la violación debe ser mayor que el daño al derecho".

“Por lo que respecta a la letra d), si las consecuencias de la medida sobre individuos o grupos son muy graves, debe demostrarse que el objetivo es de gran importancia para justificar la gravedad de las consecuencias y, si no se demuestra, la ley será inconstitucional”.

“Es en (d) donde los tribunales realizan un ejercicio de ponderación. ¿Qué es lo que se pondera? La ponderación se debe a que, por un lado, existe una ley limitativa y, por otro, un derecho o libertad constitucional. El tribunal tiene en cuenta, por un lado, el beneficio que se obtiene y, por el otro, el perjuicio. Lo que esto requiere es una evaluación de si el beneficio que se obtiene con la violación se ve compensado por la gravedad del daño causado a las personas. Si el daño causado es mayor que el beneficio, entonces la ley es inconstitucional. Este componente del examen de proporcionalidad exige que exista una relación adecuada entre el beneficio que se obtiene y el daño causado”.

“Es deber de los tribunales detallar, según surja la necesidad, los contornos completos de los derechos garantizados. [L]a aplicación estricta de [la sentencia R v Oakes 26 DLR (4th) 200] es la mejor manera de preservar los derechos y libertades fundamentales […]. El examen estricto que surge del caso Oakes hace posible un escrutinio más detallado al decir que el tribunal debe tener en cuenta cualquier efecto perjudicial de la medida en la que se confía para alcanzar el objetivo. Así, cuanto mayor sea la gravedad del efecto, más importante debe ser el objetivo y, además, debe demostrarse que la medida elegida es el medio menos perjudicial para alcanzarlo”.

“Este tipo de pensamiento no es nuevo. Como ejemplo de este enfoque me referiré al Tribunal Europeo de Derechos Humanos. Sujeto a una reserva, el dictado es aceptable. En el caso de S y otro contra el Reino Unido, en los apartados 101-102:

> 101. Una injerencia se considerará ´necesaria en una sociedad democrática´ para un fin legítimo si responde a una ´necesidad social imperiosa´ y, en particular, si es proporcionada al fin legítimo perseguido y si las razones aducidas por las autoridades nacionales para justificarla son ´pertinentes y suficientes´. Si bien corresponde a las autoridades nacionales realizar la evaluación inicial en todos estos aspectos, la evaluación final de si la injerencia es necesaria sigue estando sujeta al control del Tribunal para comprobar su conformidad con los requisitos del Convenio (véase Coster contra Reino Unido [2001] TEDH 24876/94, apartado 104, de 18 de enero de 2001, con referencias adicionales).
>
> 102. En esta apreciación, debe dejarse un margen de apreciación a las autoridades nacionales competentes. La amplitud de este margen varía y depende de varios factores, entre ellos la naturaleza del derecho del Convenio en cuestión, su importancia para el individuo, la naturaleza de la injerencia y el objeto perseguido por la injerencia. El margen tenderá a ser más estrecho cuando el derecho en cuestión sea crucial para el disfrute efectivo por el individuo de derechos íntimos o fundamentales (véase Connors contra Reino Unido [2004] TEDH 66746/01, apartado 82, 27 de mayo de 2004, con referencias adicionales). Cuando esté en juego una faceta especialmente importante de la existencia

> o la identidad de un individuo, el margen concedido al Estado será restringido (véase Evans contra Reino Unido [2007] TEDH 6339/05, apartado 77). En cambio, cuando no exista consenso en los Estados miembros del Consejo de Europa, ni sobre la importancia relativa del interés en juego ni sobre la mejor manera de protegerlo, el margen será más amplio (véase Dickson contra Reino Unido [2007] TEDH 44362/04, apartado 78)".

"Ahora expongo la reserva. El apartado 101 no refleja el examen estricto de Oakes y tampoco tiene el análisis detallado necesario que estableció Oakes. En particular, no se pregunta si la lesión del derecho es tan desproporcionada en relación con el beneficio de la ley, esto es, si es o no inconstitucional".

**4. Datos biométricos. Derecho a la intimidad. Libertad. Delitos. Niños, niñas y adolescentes.**

"[T]ratar[é] con más detalle los sistemas de identificación biométrica. Para ello me baso en la sentencia del Dr. Dhananajaya Chandrachud J en Puttaswamy (dictada el 26 de septiembre de 2018). De la lectura de las sentencias en este caso el Dr. Chandrachud J […] demostró una mayor sensibilidad a las cuestiones de intimidad y libertad que no es tan evidente en las sentencias de la mayoría o de los otros jueces que emitieron sentencias concurrentes. [Tuvo] una visión clara de los peligros de que un Estado o cualquier persona tenga control sobre la información personal:

> 121. La adopción de tecnologías biométricas en los países en desarrollo, en particular, plantea retos únicos, ya que la implantación de nuevas tecnologías en estos países rara vez va precedida de la promulgación de marcos jurídicos sólidos. Las evaluaciones de los países en los que se ha creado a posteriori un mecanismo jurídico para regular las nuevas tecnologías o proteger los datos han puesto de manifiesto que existe un enorme riesgo de violaciones masivas de los derechos humanos cuando se niegan a las personas derechos fundamentales básicos y, en casos extremos, incluso su identidad".

"[…] La NIRA ha sido aprobada. Ahora es ley, pero aún no ha entrado en vigor y, por lo tanto, aún no es operativa. El fiscal general dice que su entrada en vigor está a la espera de la finalización del marco jurídico y desde ese punto de vista esta impugnación es prematura. Respetuosamente, no puedo estar de acuerdo. [Q]ue la ley se mantenga, no sobre la base de que sea compatible con la Constitución, sino porque hay alguna otra ley por venir, eso sería una grave dejación de funciones por parte de los tribunales para tratar si la ley promulgada es conforme con la Constitución.

El Dr. Chandrachud J continuó en los párrafos 122—127:

> 122. […] La otra cara de la moneda es la preocupación por el abuso de las nuevas tecnologías, incluida la biometría, por parte del Estado y de entidades privadas mediante acciones como la vigilancia y la elaboración de perfiles a gran escala […].
>
> 124. La proliferación de la tecnología biométrica ha facilitado la invasión de la intimidad individual a una escala sin precedentes. La información en bruto que constituye el núcleo de la biometría es personal por su propia naturaleza […]. Aunque la tecnología biométrica plantea algunos de los mismos problemas que surgen cuando las agencias gubernamentales o las empresas privadas recopilan cualquier información personal

> sobre los ciudadanos, hay características específicas que distinguen los datos biométricos de otros datos personales, lo que hace que las preocupaciones sobre la tecnología biométrica sean de particular importancia en lo que respecta a la protección de la intimidad.
>
> 126. […] Sin embargo, la biometría con fines de autenticación e identificación es diferente, ya que no tiene un objetivo específico de encontrar rastros relacionados con un delito, sino que se lleva a cabo con el fin de generar información de identidad específica de un individuo. Esta diferencia de finalidad hace que la recogida de datos biométricos físicos constituya una violación más grave de la integridad y la intimidad".

"[U]na cosa es recopilar datos biométricos en el contexto de una investigación y enjuiciamiento penales y otra muy distinta es llevar a cabo una amplia recopilación de datos biométricos fuera de ese contexto. La razón es que, en general, existen disposiciones amplias y detalladas sobre la recogida y el uso de información biométrica en el contexto del derecho penal. Hasta ahora, en el contexto de la recogida general de datos biométricos fuera del contexto del derecho penal, es probable que se produzcan violaciones de los derechos fundamentales a menos que existan salvaguardias muy estrictas y rigurosas, ya que una vez que se produce una violación de la base de datos es poco probable que la información obtenida se recupere en su totalidad. Hay que recordar también que en el mundo moderno los datos no tienen que ser eliminados físicamente, sino simplemente copiados, y una vez copiados no hay límite al número de copias posteriores que pueden hacerse".

"Este último extracto plantea la controvertida cuestión de quién tiene derechos sobre los datos. ¿Es el responsable del tratamiento o es el interesado? El individuo, hasta que fue obligado por ley, tenía pleno control sobre sus datos biométricos y biográficos. La NIRA está arrebatando esta opción no sólo a los adultos, sino también a todos los niños. De hecho, el padre o la madre del niño deben solicitar su registro. Y no sólo eso, no hay opción de exclusión. Por lo tanto, si el niño desea no participar en el sistema de registro, no tiene otra opción. Ese niño ha perdido el control sobre su información biométrica para siempre".

"[Se destaca] el riesgo del efecto combinado de la tecnología con el control sobre los datos. A diferencia de la mayoría en Puttaswamy (26 de septiembre de 2018), que parecía haber adoptado una visión bastante benigna de este aspecto de la cuestión, el Dr. Chandrachud J. destruyó la noción de que simplemente porque una información similar o idéntica ya está en posesión del Estado, eso en sí mismo hace que la toma de dicha información sea legítima de nuevo. [Se] comprendió claramente las implicaciones de recopilar información biográfica, combinarla con datos biométricos y automatizar el proceso con algoritmos de apoyo. A ello se añade la posibilidad de elaborar perfiles. Este escenario se traduce en un gran poder sobre la vida de las personas, especialmente cuando esos datos y esa tecnología están en manos del Estado y de poderosos actores privados como Google, Amazon y similares. Por supuesto, con estos últimos, la participación es consentida o, como mínimo, la persona puede optar por no participar después de algún tiempo. Lo que propone la NIRA es el control de grandes cantidades de datos, sin exclusión voluntaria y vinculando los datos almacenados en diferentes silos [de datos informáticos] mediante un número de identificación único, lo que reduce aún más el anonimato

y aumenta la posibilidad de elaborar perfiles y generar nueva información sobre el titular de los datos".

"La combinación de todos esos datos con algoritmos en la era de la inteligencia artificial permite ahora generar hechos que de otro modo no se conocerían sobre el individuo y esos hechos no son relevantes para el propósito de la identificación. Estamos en la era de las máquinas ´autodidactas´, es decir, máquinas que pueden crear por sí mismas nuevos conocimientos sin necesidad de programación. Estas máquinas son capaces de hacerlo a partir de los datos que ya tienen. Respetuosamente, la mayoría en Puttaswamy (26 de septiembre de 2018) no parecía tener una comprensión completa de esto y sus implicancias, cosa que ha sido demostrado por el Dr. Chandrachud J.".

"[C]uando esta identificación única procedente de los datos biométricos se combina con un número de identificación único que se introduce en múltiples bases de datos y se rastrea el uso de ese número único, ´los datos biométricos no sólo permiten rastrear a las personas, sino que crean la posibilidad de recopilar la información de un individuo e incorporarla a un perfil completo mediante la conexión de varias bases de datos´".

"El requisito obligatorio en virtud de la NIRA requerirá que la persona comparezca en algún lugar y en algún momento no sólo para dar información biográfica, sino también para dar información biométrica y esto, según [la Corte canadiense en Blencoe v British Columbia (Human Rights Commission) 190 DLR (4th) 513], entra dentro del interés de libertad protegido por la frase ´vida, libertad y seguridad de la persona´ (énfasis añadido). La propia obligación de facilitar información biométrica afecta al interés de la libertad. Así pues, a primera vista, es probable que se infrinja el artículo 13 (3) (a) de la Carta de Jamaica si la ley entra en vigor en su estado actual. Se está privando a la persona de la posibilidad de decidir si desea facilitar información biométrica. También se le obliga a entregar su cuerpo en un lugar y a una hora determinados para que se recoja la información biométrica. La libertad de movimiento de la persona se ve limitada por el mero hecho de ser obligada a acudir a un lugar específico para facilitar la información requerida en virtud de la NIRA. El propio acto de tomar la información biométrica es una injerencia en el cuerpo de la persona".

**5. Igualdad. Asistencia social. Residencia. Derecho a la libre circulación. Servicios públicos. Prestación de servicio.**

"[E]s interesante observar que en el caso Puttaswamy (septiembre de 2018) que tenía más de mil millones de personas registradas, como información demográfica solo se requería (a) nombre; (b) fecha de nacimiento; (c) género; (d) dirección residencial. Esto contrasta fuertemente con la extensa información biográfica requerida en el Tercer Anexo de la NIRA. Además, la información recopilada no se procesó con fines económicos y sociológicos. Asimismo, el gobierno indio presentó al tribunal numerosas pruebas que sugerían que aproximadamente la mitad del dinero gastado en programas de asistencia social y de otro tipo no llegaba a los destinatarios previstos. También había pruebas de que ´sólo 15 de cada 100 rupias llegan a la persona destinataria´. Esto fue confirmado por un estudio formal (párrafo 79 de la sentencia de Ashok Bhushan J.). Señalo esto para mostrar la naturaleza y calidad de las pruebas presentadas en el caso Puttaswamy. Por

el contrario, en este caso el Estado no ha presentado prácticamente ninguna prueba de ningún tipo".

"El sistema Aadhaar era voluntario y estaba dirigido a personas concretas que necesitaban asistencia gubernamental. La NIRA, en cambio, es un sistema nacional obligatorio que se aplica a todos los jamaiquinos y residentes ordinarios, sin excepción".

"[L]as personas inscribibles, que no tengan NIN ni NIC, no podrán acceder a los servicios públicos ni siquiera comerciar en el sector privado. También vulnera el derecho a la igualdad ante la ley (artículo 13 (3) (g) de la Constitución). Además, en la medida en que se convierte en un requisito previo para el derecho a un pasaporte, afecta directamente a la libertad de circulación. Estoy de acuerdo con las alegaciones del demandado de que nada en la ley sugiere que afecte al derecho a registrarse como elector. Si se aplicara de forma que impidiera el derecho de voto, contravendría la Constitución. El derecho de voto no es un ´bien o servicio´ prestado por un organismo público".

"La actitud del Tribunal Supremo de la India ante el intento de hacer del número [único de identidad] Aadhaar un requisito previo para las transacciones comerciales es ilustrativa. El Tribunal anuló la parte de la legislación que permitía a las empresas y a los particulares solicitar la autenticación (apartado 218 de la sentencia mayoritaria). Era inconstitucional en la medida en que permitía a los intereses del sector privado exigir la autenticación mediante el número [único de identidad] Aadhaar (apartado 447(4) (h) de la sentencia mayoritaria). El Tribunal también limitó el significado de la palabra ´prestaciones´ a: programas de bienestar proporcionados por el Estado, dirigidos a una clase desfavorecida y pagados con cargo al fondo consolidado (apartado 321 de la sentencia mayoritaria). Con respecto a la educación de los niños, el tribunal decidió que la educación pública no es ´ni un servicio ni una subvención´ (apartado 332 (c) de la sentencia mayoritaria). Es manifiesto que la NIRA ofende estos planteamientos. Coaccionar a todos los ciudadanos para que obtengan un NIN y un NIC, privándoles de los servicios públicos si no lo hacen, es desproporcionado en relación con cualquier beneficio que se obtenga. El artículo 41 es inconstitucional y no puede mantenerse, ya que vulnera los derechos a la intimidad y a la libertad del sujeto y no está justificado en una sociedad libre y democrática".

"No cabe duda de que si uno decide acceder a los servicios públicos normalmente es necesario satisfacer a esa entidad sobre su identidad. Esto no es lo que hace que el artículo 41 sea ofensivo. El artículo 41 es inconstitucional porque pretende hacer de un documento nacional de identidad o de un número el único método de verificación de la identidad. Esto, por las razones adumbradas anteriormente, no está justificado en una sociedad libre y democrática".

# 2.2. TRIBUNAL DE APELACIONES DEL NOVENO CIRCUITO DE LOS ESTADOS UNIDOS DE NORTEAMERICA, "PATEL V. FACEBOOK". N° 18—15982. 8/08/2019.

## HECHOS

En 2010, Facebook presentó la herramienta "sugerencia de etiquetas" que utilizaba un Sistema de Reconocimiento Facial para identificar personas en las fotografías que los usuarios cargaban a Facebook libremente.

En 2015, un grupo de usuarios presentó una demanda colectiva en virtud de la Ley de Privacidad de la Información Biométrica de Illinois ("BIPA", siglas en inglés) ante el Tribunal de Distrito para el Norte de California, con el objetivo de impugnar la recopilación de información facial biométrica sin consentimiento previo que utilizaba la red social "Facebook". Los usuarios afectados alegaron que el sistema de sugerencias funcionaba mediante un proceso de reconocimiento facial de cuatro pasos. Primero, el sistema detectaba los rostros de las imágenes que se cargaban. Luego, la herramienta estandarizaba o "alineaba" los rostros según un conjunto de parámetros (distancia entre los ojos, la nariz y las orejas). En el tercer paso, el sistema calcula una "firma facial", que es una cadena de números que representa ese rostro en particular. Luego, el sistema busca una coincidencia en una base de datos de "plantillas faciales" almacenadas en la red social. Las plantillas faciales almacenadas se calculaban en función de otras fotografías en las que se había etiquetado a un usuario. De esa manera se producía una coincidencia cuando la firma facial caía dentro de un umbral de similitud con una de las plantillas faciales almacenadas. Esto le permitía a "Facebook" sugerir etiquetar al usuario al que le pertenece la plantilla facial.

El Tribunal de Distrito de los Estados Unidos para el Norte de California hizo lugar a la demanda colectiva presentada por el grupo de usuarios. La defensa de "Facebook" apeló la medida ante el Tribunal de Apelaciones del Noveno Circuito con sede en California. Alegó que los demandantes no habían acreditado ningún perjuicio concreto, y que solo almacenaba plantillas faciales y no firmas faciales.

## DECISIÓN

El Tribunal de Apelaciones del Noveno Circuito hizo lugar a la demanda colectiva. Consideró que el desarrollo de una plantilla de rostro o mapa facial a través del uso del Sistema de Reconocimiento Facial sin consentimiento invade la intimidad y los intereses concretos de los usuarios.

## ARGUMENTOS

### 1. Derecho a la intimidad. Sistema de Reconocimiento Facial. Protección de datos personales.

"Al abordar estos argumentos, examinamos en primer lugar ´si las disposiciones legales en cuestión se establecieron para proteger intereses concretos´ (del demandante) (en

contraposición a derechos puramente procesales)´ *Dutta v. Sate Farm Mut. Auto. Ins*. Co., 895 F3d 1166, 1174 (9th Cir. 2018) (citando *Spokeo II*, 867 F. 3d en 1113) […]".

"[Los] derechos a la intimidad del *common law* están entrelazados con zonas de intimidad personal protegidas constitucionalmente. Véase *Gibson v. Fla. Legislative Investigation Comm*., 372 U.S. 539, 569 n.7 (1963) (Douglas, J. concurre) (´Una parte de la base filosófica de [el derecho a la intimidad de la Primera Enmienda] tiene sus raíces en el *common law*´); véase también *Kyllo v. United States*, 533 U.S. 27, 34 (2001) […]".

"La Corte Suprema ha reconocido que los avances de la tecnología pueden aumentar el potencial de intromisiones irrazonables en la intimidad personal. Estas preocupaciones se extienden a las imágenes térmicas que mejoran los sentidos (ver *Kyllo*, 533 U.S. en 34; Monitoreo GPS para períodos prolongados, ver Estados Unidos contra Jones, 565 U.S. 400, 416, 428 (2012) (Sotomayor, J., y Alito, J.) (cinco jueces coinciden en que las preocupaciones de intimidad se plantean por dicho monitoreo, *Carpenter v. United States*, 138 S. Ct. 2206, 2215 (2018)); almacenamiento en teléfonos móviles modernos de ´grandes cantidades de información personal´ (*Riley v. California*, 573 U.S. 373, 386 (2014)); y avances tecnológicos en el seguimiento de la ubicación de los celulares (ver *Carpenter*, 138 S. Ct. at 2215). Los avances tecnológicos proporcionan "acceso a una categoría de información que de otro modo sería incognoscible" […], e ´implican preocupaciones de privacidad´ de una manera tan diferente de las intromisiones tradicionales como "un paseo a caballo" es distinto a ´un vuelo a la luna´(*Riley*, 573 U.S. at 393)".

"Conforme a los antecedentes históricos y los precedentes de la Corte Suprema sobre los avances tecnológicos y la intromisión sobre el derecho a la privacidad, consideramos que una intromisión o invasión de la privacidad biométrica de un individuo ´tiene una estrecha relación con un daño que tradicionalmente se ha considerado como base para una demanda […]´ (*Spokeo I*, 136 S. Ct. at 1549). ´[T]anto el *common law* como la comprensión literal de la intimidad abarcan el control por parte de un individuo de la información relativa a su persona´ (*Reporters Comm*., 489 U.S. at 763). Como en el contexto de la Cuarta Enmienda, la tecnología de reconocimiento facial que aquí se cuestiona puede obtener información "detallada, enciclopédica y recopilada con facilidad", lo que sería casi imposible sin dicha tecnología. (*Carpenter*, 138 S. Ct. at 2216). Una vez que se crea una plantilla de rostro de un individuo, Facebook puede usarla para identificar a esa persona en cualquiera de los otros cientos de millones de fotos cargadas en Facebook cada día, así como también determinar cuándo ese individuo estuvo presente en una ubicación específica. Facebook también puede identificar a los amigos o conocidos del individuo [en la red social] que están presentes en la foto. Teniendo en cuenta el desarrollo futuro de dicha tecnología como se sugiere en *Carpenter*, ver 138 S. Ct. at 2216, parece probable que un individuo con un mapa facial pueda identificarse a partir de una fotografía de vigilancia tomada en la calle o en los edificios. O se podría utilizar una plantilla facial biométrica para desbloquear el bloqueo de reconocimiento facial en el teléfono celular de esa persona. Concluimos que el desarrollo de una plantilla facial utilizando tecnología de reconocimiento facial sin consentimiento (como se alega aquí) invade los asuntos privados y los intereses concretos de un individuo […]".

"La sentencia de la Asamblea General de Illinois, que es ´instructiva e importante´ para nuestra investigación sobre la legitimación, Spokeo II, 867 F. 3d en 1112 (cita omitida), apoya la conclusión de que la captura y el uso de la información biométrica de una persona invade intereses

concretos. Como se ha señalado anteriormente, al promulgar la ley BIPA, la Asamblea General consideró que el desarrollo y uso de datos biométricos presentaban riesgos para los ciudadanos de Illinois, y que ´el bienestar´, la seguridad y la protección pública se verán favorecidos mediante la regulación de la recolección, el uso, la salvaguarda, la manipulación, el almacenamiento, la conservación y la destrucción de identificadores e información biométrica. 740 III. Comp. Stat. 14/5(g). Interpretando la ley, el Tribunal Supremo de Illinois concluyó que: ´[l]a estrategia adoptada por la Asamblea General mediante la promulgación de la ley BIPA´ era la de proteger la ´privacidad biométrica´ de las personas mediante (1) ´la imposición de salvaguardas para garantizar que los derechos de intimidad de las personas y los clientes en sus identificadores biométricos y la información biométrica se honren y protejan adecuadamente para empezar, antes que estén o puedan estar comprometidos´, y (2) ´sometiendo a las entidades privadas que no sigan los requisitos de la ley a una responsabilidad potencial sustancial´. *Rosenbach*, 2019 IL 123186, en *6—7. Sobre la base de interpretación, el Tribunal Supremo de Illinois concluyó que un individuo podría ser ´agraviado´ por una violación de la BIPA siempre que ´una entidad privada no cumpla con uno de los requisitos de la sección 15´, porque ´esa violación constituye una invasión, menoscabo o denegación de los derechos legales de cualquier persona o cliente cuyo identificador biométrico o información biométrica sea objeto de la violación´ *Id.* en *6. No es necesario que las personas sufran un ´perjuicio indemnizable más allá de la violación de sus derechos legales para que puedan interponer un recurso´. *Id*. en *7".

"Por lo tanto, concluimos que ´las disposiciones legales en cuestión´ en la BIPA se establecieron para proteger los ´intereses concretos´ de un individuo en la intimidad, no meramente los derechos procesales. Spokeo II, 867 F. 3d en 1113".

"[Respecto] a la cuestión de ´si las violaciones procesales específicas que fueron alegadas en este caso realmente perjudican, o presentan un riesgo material de perjudicar dichos intereses´. *Spokeo II*, 867 F. 3d en 1113. La conducta relevante de Facebook, según la demanda, es la recopilación, uso y almacenamiento de identificadores biométricos sin una autorización por escrito, en violación de la sección 15(b), y la falta de mantenimiento de un calendario de conservación o directrices para la destrucción de identificadores biométricos, en violación de la sección 15(a).[8] Los demandantes alegan que una violación de estos requisitos permite a Facebook

[8] Los artículos 15 (a) y (b) de la BIPA establecen: (a) Una entidad privada en posesión de identificadores biométricos o información biométrica debe desarrollar una política escrita, puesta a disposición del público, que establezca un calendario de conservación y directrices para destruir permanentemente los identificadores biométricos y la información biométrica cuando se haya cumplido el propósito inicial de recopilar u obtener dichos identificadores o información o en un plazo de 3 años a partir de la última interacción del individuo con la entidad privada, lo que ocurra primero. En ausencia de una orden o citación válida emitida privada en posesión de identificadores o información biométricos deberá cumplir su calendario de conservación y directrices de destrucción establecidos; (b) Ninguna entidad privada podrá recoger, capturar, comprar, recibir a través del comercio u obtener de otro modo el identificador biométrico o la información biométrica de una persona o de un cliente, a menos que primero: (1) informe por escrito al sujeto o a su representante legalmente autorizado de que se está recogiendo o almacenando un identificador biométrico o información biométrica; (2) informe por escrito al sujeto o a su representante legalmente autorizado de la finalidad y duración de la recopilación, almacenamiento y utilización de un identificador biométrico o de información biométrica; y (3) reciba una autorización por escrito firmada por

crear y utilizar una plantilla facial y conservarla para siempre. Dado que el derecho a la intimidad protegido por la BIPA es el derecho a no estar sujeto a la recogida y uso de tales datos biométricos, la supuesta violación de Facebook de estos requisitos legales violaría necesariamente los intereses sustantivos de intimidad de los demandantes. Como explicó el Tribunal Supremo de Illinois, las protecciones procesales de la BIPA ´son particularmente cruciales en nuestro mundo digital´ porque ´[c]uando una entidad privada no se atiene a los procedimientos legales… el derecho del individuo a mantener su intimidad biométrica se desvanece en el aire´. *Rosenbach*, 2019 IL 123186, en *6 (depurado). En consecuencia, concluimos que los demandantes han alegado un perjuicio concreto de hecho suficiente para conferir la legitimación del artículo III".

"Dada la naturaleza de la supuesta infracción de la BIPA, el recurso de Facebook a *Basset v. ABM Parking Services*, Inc. 883 F. 3d en 780, [que el demandante no había alegado un perjuicio concreto] está fuera de lugar "[…] la supuesta recopilación, uso y almacenamiento por parte de Facebook de las plantillas de rostros de los demandantes y las violaciones de los procedimientos de la BIPA realmente dañan o suponen un riesgo material de daño a esos intereses de privacidad, véase *Dutta*, 895 F. 3d en 1174, los demandantes han alegado un daño concreto y particularizado, suficiente para conferir legitimación al amparo del artículo III".

el sujeto de identificador biométrico o de la información biométrica o por el representante legalmente autorizado del sujeto.

# 2.3. TRIBUNAL DE JUSTICIA DEL ESTADO DE SAN PABLO, "IDEC V. CONCESIONARIA DE LA LÍNEA 4 DEL METRO DE SAN PABLO (VIAQUATRO)". 7/05/2021.

**HECHOS**

En 2018, la empresa "Via Quatro", operador de la concesionaria responsable de la Línea 4 del Metro de San Pablo, instaló puertas interactivas en algunas estaciones con el objetivo de proyectar anuncios personalizados a los pasajeros, así como también para recabar información que pudiera servir en la medición de información demográfica y analizar la reacción emocional de los usuarios del servicio por intermedio de cámaras equipadas con tecnología de reconocimiento facial.

Ante esta situación, el Instituto Brasilero de Defensa del Consumidor (IDEC) —organismo de protección de los derechos del consumidor— junto a la oficina de los defensores públicos del Estado de San Pablo, presentaron una acción colectiva ante un juzgado civil del mismo lugar con la pretensión de que, como medida cautelar, la empresa concesionaria deje de recopilar datos de los puertos interactivos digitales y que confirme la desconexión de las cámaras ya instaladas, bajo pena de multa diaria de $50.000 reales. Además, solicitó que se condene a la empresa concesionaria a no utilizar datos biométricos o cualquier otro tipo de identificación de consumidores y usuarios del transporte público; a pagar una indemnización por la utilización indebida de la imagen de los consumidores, y por daños colectivo en un valor no inferior a los 100 millones de reales brasileños.

**DECISIÓN**

El Juzgado Civil N° 37 del Estado de San Pablo, confirmó la medida cautelar que había sido otorgada y ordenó a la empresa concesionaria que se abstuviera de captar imágenes, sonidos y cualquier otro dato personal de los usuarios consumidores a través de cámaras u otros dispositivos, sin el consentimiento previo del consumidor. Además, determinó que si la empresa deseaba hacer uso del sistema debía obtener el consentimiento previo de los usuarios a través de información clara y específica sobre las captura y procesamiento de datos, con la adopción de herramientas pertinentes; y la condenó a pagar una indemnización por daños morales colectivos por $100.000 reales.

**ARGUMENTOS**

1. **Protección de datos personales. Usuarios y Consumidores. Reconocimiento fotográfico. Sistema de Reconocimiento Facial. Carga de la prueba. Informe pericial.**

"[N]o existen dudas de que el peritaje se produjo en [otro expediente] sin que haya existido participación del demandante, así como del Ministerio Público, la Defensoría del Pueblo y los *amicus curiae*, que son parte de este litigio. [...] Por tanto, la prueba ofrecida es inadmisible, ya que su aceptación implicaría una limitación real de la defensa, ya que la demandante y los demás involucrados no participaron en su elaboración, no tuvieron oportunidad de formular preguntas ni indicar asistentes técnicos, y estaban expresamente en desacuerdo con el uso del informe.

La [empresa] demandada, por su parte, defiende la legalidad del uso del equipo en cuestión, argumentando que no existe recolección ni almacenamiento de datos personales en el sistema, sino sólo detección de rostros con fines estadísticos, por lo que los datos generados no identifican específicamente el pasajero. [...] Sucede, sin embargo, que tal limitación del sistema de utilizar únicamente las imágenes de los usuarios con fines estadísticos, sin captura, registro o identificación efectiva no ha sido demostrado en el expediente, carga que correspondía al demandado [...]".

"Ante el hecho incontrovertible de que existían equipos de grabación de imágenes de usuarios con fines publicitarios y estadísticos en emisoras gestionadas por [la empresa], [le] correspondía […] como concesionario de un servicio público, demostrar plenamente que el sistema [de inteligencia artificial] no almacena datos personales de los usuarios de la plataforma, ni realiza el reconocimiento facial a través del equipo instalado, la ausencia de grabación o filmación de los usuarios y el destino real dado al material obtenido, en su caso, lo que no se produjo".

"Se puede advertir que [el concesionario], en más de una oportunidad, dejó de solicitar la realización de testeos en los equipos y sistemas operativos vinculados, prueba esencial para demostrar sus alegaciones, requiriendo única y genéricamente el uso como prueba del informe pericial elaborado en [otro expediente], elemento de prueba que fue declarado inadmisible [...]. Y aunque no fuera así, [d]el informe [declarado inadmisible] se concluye que se realizó únicamente un peritaje indirecto, sin que hubiera habido un examen de los equipos reales y específicos y de los respectivos sistemas operativos en cuestión […]. Al no haber un interés por parte de la empresa concesionaria en demostrar concretamente el destino real dado a la información inequívocamente recolectada como titular de los equipos instalados en las instalaciones de las estaciones de la Línea 4, se concluye que no ha demostrado las razones que justifiquen la medida".

"Incluso si se comprobara concretamente la ausencia de reconocimiento facial efectivo a través del equipo instalado, no cabe dudas que existen capturas de imágenes de los usuarios, sin su conocimiento o consentimiento para fines comerciales que benefician a la empresa concesionaria y a la empresa contratado por ella. [La empresa demandada] confiesa que se detecta la imagen de los usuarios y que dichos datos se utilizan para fines estadísticos […]. Por tanto, no existe controversia sobre la detección de imágenes de los usuarios, así como la captura y reconocimiento de información como género, franja etaria, reacción a la publicidad emitida, entre otros".

## 2. Protección de datos personales. Sistema de Reconocimiento Facial. Datos biométricos. Defensa del consumidor. Derecho a la intimidad. Derecho a la imagen.

"El reconocimiento facial o incluso la mera detección facial, sin que la identificación concreta del individuo sea posible, pero con acceso a su imagen y rostro, ya parece toparse con el concepto de dato biométrico, considerado jurídicamente como dato personal sensible, por lo que merece un tratamiento especial […]."

"Cabe señalar que [la legislación brasilera de protección de datos personales] estableció una protección especial para los datos personales sensibles, autorizando su tratamiento sólo en caso

de consentimiento claro y específico por parte del titular de los datos o, sin el consentimiento del titular, en las situaciones enumeradas en la legislación interna […] Además, la finalidad del tratamiento debe tener fines legítimos, específicos, explícita e informada al titular, sin posibilidad de procesamiento posterior incompatible con estos fines […]".

"La situación expuesta en el caso concreto es muy diferente a la captura de imágenes por sistemas de seguridad con el objetivo de mejorar la prestación del servicio, la seguridad de los usuarios o mantenimiento del orden, lo cual sería no sólo aceptable, sino necesario dada la obligación del prestador de servicios públicos de garantizar la seguridad de sus usuarios dentro de sus instalaciones. Es evidente que la captura de imagen en este caso se utiliza con fines publicitarios y posterior carácter comercial, ya que, en líneas generales, se busca detectar las principales características de los individuos que circulan en determinados lugares y épocas, así como sus emociones y reacciones frente a la publicidad transmitida en los equipos […]. Además, es indiscutible que los usuarios no fueron advertidos ni comunicados previa o posteriormente sobre el uso o captura de su imagen por tótems instalados en las plataformas, es decir, los usuarios ni siquiera son conscientes de la práctica llevada a cabo por la empresa concesionaria lo cual viola claramente su derecho a tener información sobre productos y servicios, así como la protección contra publicidad engañosa y métodos comerciales abusivos, coercitivos o desleales, ambos enumerados en la [Ley de protección al consumidor]".

**3. Obligaciones de hacer. Consentimiento informado. Derecho a la imagen.**

"[L]a conducta de la empresa concesionaria viola manifiestamente el derecho a la imagen de los consumidores que utilizan el servicio público, las disposiciones relativas a la protección especial dada a los datos personales sensibles recabados, además de la violación de derechos básicos de los consumidores, en particular información y protección en relación con prácticas comerciales abusivas, de ahí que sea válida la solicitud de una obligación de no hacer que consiste en no utilizar datos biométricos o cualquier otro tipo de identificación de consumidores y usuarios del transporte público sin acreditar el debido consentimiento del consumidor".

"Si el demandado decidiera volver a adoptar prácticas como las tramitadas en este expediente deberá obtener el consentimiento previo de los usuarios a través de la información clara y específica sobre la captura y procesamiento de los datos, con la adopción de las herramientas pertinentes a tales fines".

**4. Daño. Indemnización.**

"Es importante señalar que la reparación moral colectiva se acepta como una forma de indemnización por el daño sufrido por la comunidad, alejándose, a priori, del concepto de daño moral individual. Esto significa que no se confundan daños individuales homogéneos y colectivos, siendo completamente posible, en teoría, la coexistencia de los dos tipos de daño. [...] Sin embargo, aunque el demandante ha presentado una demanda de daños y perjuicios que reclama autonomía e independientes entre sí, la duplicidad no se produce en el caso concreto, porque la pretensión daño moral a la comunidad de personas que visitaron el [la línea de metro] de la demandada, ciertamente se confunde con el daño moral colectivo previsto en el caso concreto".

“En este caso, la posibilidad de reconocimiento facial, detección facial, uso de imágenes capturadas de usuarios del metro, con un evidente propósito comercial, así como la ausencia de autorización previa o de mero conocimiento científico para captar la imágenes, revela conductas bastante reprobables capaces de afectar la moral y los valores colectivos, especialmente considerando el incalculable número de individuos que pasan por [la línea de metro a cargo de la empresa demandada] a diario, incluidos niños y adolescentes, cuya imagen goza mayor y notoria protección [...]”.

“El monto pretendido por el autor $100.000.000 de reales es sumamente excesivo, porque se desvía de los parámetros señalados anteriormente y no es consistente con el daño sufrido por la comunidad, principalmente porque no hay constancia en los registros de que las imágenes han sido compartidas y almacenadas permanentemente o publicadas en medios de fácil y amplia difusión de la comunicación”.

# 2.4. TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH), "GLUKHIN V. RUSIA". CASO N° 11519/20. 4/7/2023.

**HECHOS**

Un hombre realizó una manifestación pacífica en un subterráneo de Moscú, donde sostuvo una figura de cartón de un reconocido activista y opositor político. El Código de Infracciones Administrativas (el CAO) de Rusia, requiere que las personas notifiquen a las autoridades antes de realizar manifestaciones públicas con determinados objetos. Diferentes Imágenes y videos de la demostración circularon a través del sistema de mensajería Telegram. La unidad antiextremismo de la policía rusa utilizó esas imágenes para identificar al hombre. De esta manera, días más tarde, a través de las cámaras de seguridad del subterráneo de Moscú, la policía rusa localizó y detuvo al manifestante. El hombre fue procesado por la falta administrativa. En el marco del proceso, la policía utilizó capturas de las imágenes que habían circulado en redes sociales y las grabaciones de las cámaras de seguridad del subterráneo ruso. El hombre alegó que la utilización de las tecnologías de identificación por parte de la policía era ilegal y, además, que su manifestación pacífica estaba protegida bajo la libertad de expresión. El Tribunal del distrito Meshchanskiy de Moscú consideró que el hombre había incumplido la reglamentación aplicable y lo condenó al pago de una multa. La persona condenada apeló la decisión. Para ello, consideró que el procedimiento realizado por la unidad antiextremismo había sido ilegal, toda vez que la Ley de actividades de búsqueda operativa (la OSAA) no autorizaba el uso de tecnologías de reconocimiento facial para investigar infracciones administrativas. Sin embargo, su reclamo no tuvo éxito.

**DECISIÓN**

El Tribunal Europeo de Derechos Humanos consideró que Rusia era responsable por la violación de los artículos 8 (vida privada y familiar) y 10 (libertad de expresión) del Convenio Europeo de Derechos Humanos.

**ARGUMENTOS**

1. **Sistema de Reconocimiento Facial. Fuerzas de seguridad. Derecho a la privacidad. Derecho a la vida privada y familiar. Protección de datos personales. Espacio público. Cámara de seguridad. Medidas de seguridad. Principio de legalidad.**

"[El Tribunal] reitera que el concepto de ´vida privada´ es un término amplio no susceptible de definición exhaustiva. Puede abarcar múltiples aspectos de la identidad física y social de la persona. No se limita a un ´círculo íntimo´ en el que el individuo puede vivir su propia vida personal sin interferencias externas, sino que también abarca el derecho a llevar una ´vida social privada´, es decir, la posibilidad de establecer y desarrollar relaciones con otras personas y con el mundo exterior. No excluye las actividades que tienen lugar en un contexto público. Existe, pues, una zona de interacción de una persona con otras, incluso en un contexto público, que puede entrar en el ámbito de la ´vida privada´ (véase TEDH, López Ribalda y otros c. España, párrafos 87-88)" (cfr. párr. 64).

El simple almacenamiento de datos relativos a la vida privada de una persona equivale a una injerencia en el sentido del artículo 8. El uso posterior de la información almacenada no influye en esta conclusión. Sin embargo, para determinar si la información personal retenida por las autoridades implica alguno de los aspectos de la vida privada […], el Tribunal tendrá debidamente en cuenta el contexto especifico en el que se ha registrado y retenido la información en cuestión, la naturaleza de los registros, la forma en que estos se utilizan y procesan los registros y los resultados que pueden obtenerse (véase TEDH, S. y Marper c. Reino Unido, párrafo 67)" (cfr. Párrafo 65).

El registro sistemático o permanente de datos personales [a través de dispositivos de fotografía o video] puede implicar cuestiones de privacidad, en especial cuando se trata de fotografías de una persona identificada. La imagen de una persona constituye uno de los atributos principales de su personalidad, dado que revela sus características únicas y la distingue de sus pares. El derecho de toda persona a la protección de su imagen es por ende un elemento esencial del desarrollo personal y presupone el derecho a controlar la utilización de su imagen. Si bien en la mayoría de los casos esto significa la posibilidad del individuo de negarse a la publicación de su imagen, también implica el derecho a oponerse al registro, conservación y reproducción de su imagen por parte de terceros" (cfr. párr. 66).

El Tribunal ha declarado anteriormente que la recolección y almacenamiento de datos por parte de las autoridades sobre personas concretas constituía una intromisión en la vida privada de esas personas, incluso si esos datos se referían exclusivamente a las actividades públicas de la persona (Cfr. TEDH, Amann c. Suiza, párrafos 65-67, y Rotaru v. Rumania, párrafos 43-44), como la participación en manifestaciones antigubernamentales (véase TEDH, Asociación ´21 de diciembre de 1989´ y otros v. Rumania, párrafo 170, así como también en Catt v. Reino Unido, párrafo 93). Asimismo, ha considerado que los siguientes supuestos de recolección de datos en un lugar público constituían una injerencia en la vida privada de las personas: la grabación de un interrogatorio en una zona pública de una comisaría de policía (véase TEDH, P. G. y J. H. c. Reino Unido, párrafos 56-60); la grabación por cámaras de videovigilancia en un lugar público y la posterior divulgación de las imágenes de video a las medios de comunicación (véase TEDH, Peck c. Reino Unido, párrafos 57-63); la grabación de imágenes de video en una comisaría de policía y su posterior utilización en procedimientos penales (véase TEDH, Perry c. Reino Unido, párrafos 36-43); la recolección de datos a través de un dispositivo GPS conectado al auto de una persona, y el almacenamiento de datos relativos al paradero y los movimientos de esa persona en la esfera pública (véase TEDH, Uzun v. Alemania, párrafos 51-53, y Ben Faiza v. Francia, párrafos 53-55); el registro del nombre de una persona en una base de datos policial que recolectaba y procesaba automáticamente información sobre su desplazamiento en tren o en avión (véase TEDH, Shimovolos c. Rusia, párrafo 66); y la videovigilancia de los anfiteatros universitarios de una universidad pública (véase TEDH Antović y Mirković c. Montenegro, párrafos 40-45 y 55)" (cfr. párr. 67).

[El Tribunal señala que] durante un control rutinario de Internet, la policía descubrió fotografías y un video del solicitante celebrando una manifestación en solitario publicados en un canal público de Telegram. Hicieron capturas de pantalla del canal de Telegram, las almacenaron y supuestamente les aplicaron tecnología de reconocimiento facial para identificar al solicitante.

Tras haber identificado el lugar del video como una de las estaciones del subterráneo de Moscú, la policía recolectó grabaciones de video de las cámaras de vigilancia instaladas en dicha estación, así como en otras dos estaciones por las que había transitado el solicitante. Hicieron capturas de pantalla de dichas grabaciones de video y las almacenaron. Además, utilizaron supuestamente las cámaras de videovigilancia de reconocimiento facial en vivo instaladas en el subterráneo de Moscú para localizar y detener al solicitante varios días después con el fin de imputarle una infracción administrativa. Las capturas de pantalla del canal de Telegram y de las grabaciones de video de las cámaras de videovigilancia se utilizaron posteriormente como prueba en el procedimiento por infracción administrativa contra el solicitante" (cfr. párr. 68).

En este contexto, y teniendo en cuenta la dificultad del solicitante para probar lo que alegaba debido a que la legislación nacional no preveía un registro o notificación del uso de la tecnología de reconocimiento facial, la ausencia de cualquier otra explicación para la rápida identificación del solicitante, y el reconocimiento implícito por parte del gobierno del uso de la tecnología de reconocimiento facial en vivo, el Tribunal acepta en las circunstancias particulares del caso que se utilizó la tecnología de reconocimiento facial. El Tribunal ha considerado anteriormente que el almacenamiento de fotografías por parte de la policía, junto con la posibilidad de aplicar técnicas de reconocimiento facial en ellas, constituía una injerencia en el derecho a la vida privada (véase TEDH, Gaughran v. Reino Unido, 2020, párrafos 69-70)" (cfr. párr. 72).

El Tribunal concluye que el procesamiento de los datos personales del solicitante en el marco del procedimiento por infracción administrativa seguido contra él, incluida la utilización de la tecnología de reconocimiento facial —en primer lugar, para identificarlo a partir de las fotografías y el video ambos publicados en Telegram y, en segundo lugar, para localizarle y detenerle posteriormente mientras viajaba en el subterráneo de Moscú—, constituyó una injerencia en su derecho al respeto de su vida privada en el sentido del artículo 8, apartado 1, del Convenio" (cfr. párr. 73)".

**2. Sistema de Reconocimiento Facial. Protesta. Fuerzas de seguridad. Principio de proporcionalidad. Libertad de expresión. Libertad de asociación. Derecho a la privacidad. Derecho a la vida privada y familiar.**

"La policía recolectó y almacenó las imágenes del solicitante y las utilizó para extraer y procesar sus datos biométricos mediante tecnología de reconocimiento facial: primero, para identificarlo a partir de las fotos y videos publicados en Telegram, y luego para localizarlo y detenerlo mientras viajaba en subte. El Tribunal considera que estas medidas son particularmente intrusivas, en especial en lo que refiere al uso de tecnologías de reconocimiento facial en vivo. Por ende, el uso de estas tecnologías exige una justificación de gran relevancia para ser considerada 'necesaria en una sociedad democrática'. Asimismo, los datos personales procesados contenían información sobre la participación del solicitante en una manifestación pacífica, y por lo tanto revelaban su opinión política. Por ese motivo, estos datos recaían dentro de la categoría especial de datos sensibles que requieren un grado elevado de protección" (cfr. párr. 86).

En la evaluación de la ´necesidad en una sociedad democrática´ del procesamiento de datos personales en el contexto de las investigaciones, la naturaleza y la gravedad de los delitos en cuestión es uno de los elementos que deben tenerse en cuenta (véase, *mutatis mutandi*, TEDH,

P.N. c. Alemania, párrafo 72). La legislación nacional permite el procesamiento de datos biométricos en relación con la investigación y el enjuiciamiento de cualquier delito, con independencia de su naturaleza y gravedad" (cfr. párr. 87).

El solicitante fue procesado por una falta menor, que consistió en realizar una manifestación en solitario sin notificación previa —una falta clasificada como administrativa antes que criminal bajo la norma local— [...]. El uso de tecnología de reconocimiento facial sumamente intrusiva para identificar y detener participantes de una manifestación pacífica podría tener un efecto amedrentador ('*chilling effect*') respecto a los derechos a la libertad de expresión y asociación" (cfr. párr. 88).

En tales circunstancias, el uso de tecnología de reconocimiento facial para identificar al solicitante a partir de las fotografías y el video ambos publicados en Telegram —y, *a fortiori*, el uso de tecnología de reconocimiento facial en vivo para localizarlo y detenerlo mientras viajaba en el subterráneo de Moscú— no correspondía a una ´necesidad social apremiante´" (cfr. párr. 89).

El uso de tecnología de reconocimiento facial sumamente intrusiva contra una persona que ejerce su derecho a la libertad de expresión es incompatible con los ideales y valores de una sociedad democrática [...]. El procesamiento de los datos personales del solicitante mediante tecnología de reconocimiento facial en el marco de un proceso por una falta administrativa —primero, para identificarlo a partir de las fotos y videos publicados en Telegram y luego para localizarlo y detenerlo mientras estaba viajando en el subte— no puede ser considerado 'necesario en una sociedad democrática'" (cfr. párr. 90).

Por consiguiente, se ha producido una violación del artículo 8 del Convenio" (cfr. párr. 91)".

# 2.5. TRIBUNAL SUPERIOR DE NUEVA JERSEY. SALA DE APELACIONES. "ESTADO DE NUEVA JERSEY V. ARTEAGA". EXPEDIENTE N° A—3078—21. 7/6/2023.

**HECHOS**

En noviembre de 2019 ocurrió un robo a un local en la ciudad de Nueva York. Una de las empleadas del establecimiento manifestó haber identificado al presunto autor del hecho. La gerente de la tienda —quien no se encontraba presente en el lugar al momento de lo ocurrido—, también creyó reconocer al autor luego de revisar las cámaras de seguridad. Esa información fue utilizada por los detectives policiales que intervinieron en la averiguación del robo, quienes recuperaron las grabaciones de las cámaras de vigilancia del lugar y las de una propiedad cercana. Esas grabaciones mostraban a una persona transitando cerca del lugar el día del robo. Los agentes usaron esas filmaciones para generar una imagen fija de poca calidad que fue enviada al Centro de Inteligencia de Operaciones Regionales de Nueva Jersey (NJROIC, por su sigla en inglés) para su análisis a través del uso de tecnología de reconocimiento facial. Personal de la NJROIC informó que no existían coincidencias entre la imagen generada por los detectives y su base de datos, y que, si bien no descartaban la posibilidad de volver a realizar un posterior cotejo, requerían una imagen de mejor calidad. En su lugar, los detectives enviaron todas las imágenes de vigilancia obtenidas al Centro de Delincuencia en Tiempo Real del Departamento de Policía de Nueva York (NYPDRTCC, por su sigla en inglés). Una imagen fija seleccionada por los investigadores fue comparada con la base de datos del centro y ofreció a Francisco Arteaga como "posible coincidencia". Eso les permitió a los investigadores generar dos matrices fotográficas compuestas por fotos de otras personas y la ofrecida como posible coincidencia. Ambas matrices fueron mostradas por separado, tanto a la empleada como a la dueña del lugar, quienes identificaron a Arteaga como el autor del delito. Su defensa solicitó, entre otras cuestiones, que la fiscalía informe (se realice el llamado "*discovery*") el proveedor y el código fuente del Sistema de Reconocimiento Facial, el margen de error, la foto que se utilizó para identificar al acusado y otra información que pretendía utilizar para discutir la validez de su reconocimiento. Para fundar ese pedido, la defensa acompañó la declaración de un experto en tecnología de reconocimiento facial en la que se explicaba los principales problemas de fiabilidad de ese tipo de tecnología y porqué la defensa necesitaba que la fiscalía le revele esa información. El tribunal rechazó el pedido. Para decidir de esa manera, entre otras cuestiones, explicó que la fiscalía no tenía la obligación de producir la información solicitada por la defensa, porque el Sistema de Reconocimiento Facial no estaba bajo su cuidado, custodia o control. Ante esa decisión, la defensa interpuso un recurso de apelación.

**DECISIÓN**

El Tribunal Superior de Nueva Jersey hizo lugar al recurso de apelación solicitado por la defensa, revocó lo resuelto por el tribunal y ordenó a la fiscalía que provea (que realice el *discovery)* la información solicitada por la defensa.

**ARGUMENTOS**

**1. Prueba. Carga de la prueba. Cámara de seguridad. Acusación. Derecho de defensa. Sistema de Reconocimiento Facial.**

"[L]a prueba que se busca está directamente vinculada a la capacidad de la defensa para probar la fiabilidad de [la Tecnología de Reconocimiento Facial] [Facial Recognition Technology, FRT por su sigla en inglés]. Como tal, es indispensable para impugnar la identificación de los testigos, cuestionar la investigación del Estado, crear una duda razonable y demostrar la culpabilidad de terceros.

[El Tribunal] no está convencido de que el Centro de Delincuencia en Tiempo Real del Departamento de Policía de Nueva York no formara parte del equipo de la acusación. Esto porque el fiscal envió una solicitud a la NYPDRTCC cuya respuesta fue utilizada como elemento de acusación de [Arteaga]. Además, el fiscal obtuvo material de descubrimiento [relacionado a la FRT] por parte del NYPDRTCC […]. El Estado sostiene que no es que no pudo obtener la información adicional [datos utilizados para entrenar el RFT y la evaluación de la fiabilidad de los métodos] solicitada por la defensa, ya sea por razones de propiedad intelectual o de otro tipo, sino que la presentación de esa información le corresponde al acusado y no a él. Rechazamos esta afirmación porque la carga de la prueba recae en el Estado toda vez que la FRT resulta novedosa y no ha sido probada, y, además, porque la detección de errores de esa tecnología permitiría la exculpación de [Arteaga].

Hay pocas pruebas en el expediente sobre el software en cuestión. Sin embargo, el acusado [junto con otros actores] nos proporcionan pruebas convincentes de la novedad de la FRT, la agencia humana involucrada en la generación de imágenes, y el hecho de la veracidad de la FRT, toda vez que esa tecnología no ha sido probada o encontrada confiable por ninguna corte de Nueva Jersey".

**2. Sistema de Reconocimiento Facial. Protección de datos personales. Identificación de personas. Reconocimiento fotográfico.**

"La FRT puede detectar un rostro humano dentro de una imagen. Utiliza un algoritmo para realizar el análisis, que reconoce ´puntos nodales´ del rostro —´rasgos identificativos [distancia entre los ojos, la anchura de la nariz, la forma de los pómulos y la longitud de la mandíbula] que conforman los rasgos faciales humanos´— son comparados con los rasgos correspondientes en imágenes seleccionadas. […]. El algoritmo subyacente se desarrolla mediante aprendizaje automático que se entrena a lo largo del tiempo para reconocer posibles coincidencias pidiéndole que compare miles de imágenes con una base de datos. […]. En cada caso, el programa estima si existe una coincidencia, se le indica si el resultado es correcto y, a continuación, utiliza estos datos relativos a aciertos o fallos para informar evaluaciones posteriores, […], finalmente se centra en las características que han sido indicadores más fiables de esa coincidencia.

El proceso comienza cuando la persona que maneja el software selecciona una imagen de sondeo capturada a partir de una grabación de vigilancia en la que aparece el rostro del agresor. […]. Las imágenes de menor calidad pueden editarse para corregir la iluminación o el color, para mejorar los detalles o incluso para cambiar la expresión facial. Luego, la tecnología descompone la imagen en rasgos componentes y los destila en una ´huella facial´, un ´mapa escrito en código que mide

la distancia entre rasgos, líneas y elementos faciales´. […]. A continuación, compara esa ´huella facial´ con otras de la base de datos, asignando puntuaciones a cada una de ellas en función del grado de alineación de los rasgos correspondientes, y devolviendo una lista de aquellas con las puntuaciones más altas ordenadas por rango […].

La fiabilidad de los resultados puede depender de muchas variables encontradas a lo largo del proceso. Algunas publicaciones sugieren que la calidad y la diversidad de las imágenes utilizadas para entrenar la tecnología pueden influir en la capacidad de ésta para reconocer rostros distintos de los del conjunto inicial, lo que a menudo se traduce en un bajo rendimiento en el análisis de rostros no blancos. […]. Además, la calidad de una imagen de sondeo, incluida su resolución, iluminación ambiental y expresión facial […], así como el alcance de cualquier edición realizada en ella […] pueden afectar a la precisión de la ´huella facial´ resultante y a la capacidad del software para compararla de forma significativa con las otras huellas de la base de datos.

La defensa del acusado sostiene que la fiabilidad de la FRT depende en gran medida de su diseño y formación, así como de los parámetros utilizados por el analista que la maneja. Afirma que la búsqueda de pruebas que había solicitado resulta relevante para evaluar la fiabilidad de los resultados de la FRT utilizados para la identificación. El perito experto propuesto por la defensa explicó que el código fuente y los materiales relacionados son necesarios para analizar el diseño del software y los métodos de entrenamiento en busca de fallos estructurales inherentes al software que pudieran introducir sesgos que comprometan la exactitud de los resultados generados por el software. La fiabilidad de la tecnología implica la exactitud de las identificaciones de los testigos oculares, la minuciosidad de la investigación del Estado y la capacidad de demostrar la existencia de otros sospechosos viables. El acusado sostiene que, si no se aporta esa información [descubrimiento de la FRT], el Estado no podrá presentar las identificaciones realizadas por Vásquez-Arias y Cardozo porque ambas son el ´fruto´ de una tecnología no probada.

Rechazamos la última afirmación porque nuestro examen de los registros de la audiencia 'Wade' [audiencia previa al juicio] y la opinión del juez nos convencen de que el proceso de identificación del testigo, aunque defectuoso, no era tan irreparable como para ser inadmisible en el juicio. Lo que debe determinarse en una audiencia [previa al juicio] 'Wade' consiste en si el procedimiento de identificación presentó una ´probabilidad muy sustancial de identificación errónea irreparable´ para socavar la fiabilidad del resultado como un producto genuino de la memoria del testigo ocular en lugar de una influencia indebida. […]. El proceso de identificación se analiza a la luz de un conjunto de factores establecidos: ´variables del sistema´ bajo el control del Estado, como la administración ciega del procedimiento, las instrucciones previas al reconocimiento y la construcción y presentación de la [rueda de reconocimiento fotográfico], así como ´variables a estimar' fuera del control del Estado, como la duración y las condiciones en las que el testigo observó el evento, las características individuales del testigo o del autor que podrían influir en la memoria o la percepción, o la distancia temporal del evento […].

Aunque la construcción de la [rueda de reconocimiento fotográfico] es un factor para tener en cuenta, la preocupación con la construcción es si el sospechoso se destaca de los demás que figuran en la rueda o si la rueda incluye suficientes 'distractores' distintos del sospechoso, para garantizar que ´pone a prueba la memoria de un testigo y disminuye la posibilidad de que un

testigo simplemente esté adivinando´. […]. La razón por la que un individuo en particular es sospechoso y, en consecuencia, está incluido en el conjunto no es relevante para esa investigación. Cf. State v. Guerino, 464 N.J. Super. 589, 607 (App. Div. 2020) (en el que se concluyó que el breve comentario de un detective a la víctima de que el Estado había elaborado una rueda basada en ´fuentes de investigación´ no era indebidamente sugestivo, porque ´simplemente hizo explícito lo que entienden implícitamente los testigos que participan en un procedimiento de identificación, es decir, que debe haber alguna razón por la que la policía seleccionó las fotografías que se incluyeron en la matriz´).

Basándonos en nuestra revisión de los registros de la audiencia [previa al juicio] 'Wade' no podemos concluir que Vásquez—Arias y Cardozo se sintieran presionadas para identificar a un autor de entre las fotos de las ruedas presentadas a cada uno de ellos. El registro no apoya el argumento de que había una probabilidad sustancial de identificación errónea irreparable.

Sin embargo, la disputa sobre el descubrimiento [de la FRT] es independiente de la audiencia 'Wade' y consideramos que la solicitud de revelación de la FRT es relevante para la capacidad del acusado de impugnar la identificación y la investigación, y su capacidad general de establecer una duda razonable en el juicio. La fiabilidad de la FRT tiene implicaciones obvias para la exactitud del proceso de identificación, porque una rueda construida en torno a una coincidencia potencial errónea dejaría al testigo sin un autor real para elegir. La fiabilidad de la tecnología guarda relación directa con la calidad y la minuciosidad de la investigación penal en general, y con el hecho de si las posibles coincidencias que arrojó el programa informático permitieron obtener otros sospechosos alternativos viables para establecer la culpabilidad de terceros. La solicitud formulada por la defensa en cuanto a la identidad, diseño, especificaciones y funcionamiento del programa o programas utilizados para el análisis, y la base o bases de datos utilizadas para la comparación son relevantes para la fiabilidad del FRT.

En el juicio, es probable que el Estado haga que el agente que realizó la investigación explique la investigación policial, incluido el proceso de recuperación de la foto fija de las cámaras de vigilancia utilizada en última instancia para generar una imagen del acusado. Aunque no especulamos sobre la naturaleza exacta de este testimonio y si el acusado tratará de impugnarla, el hecho de que el Estado no tenga la carga de presentar un testimonio sobre la composición de la rueda de reconocimiento fotográfica no impide a la defensa acceder a la prueba solicitada.

En State v. Branch, la Corte Suprema sostuvo que el testimonio de por qué un ´agente colocó la fotografía del acusado en la rueda carece de relevancia para el proceso de identificación y es altamente perjudicial´. 182 N.J. 338, 352 (2005). El agente en Branch testificó que ´colocó la fotografía del acusado en una rueda fotográfica 'por la información recibida´´. […]. El Tribunal consideró que esto era problemático porque ´se basaba en prueba *hearsay* inadmisible. Implicaba que el agente de policía tenía información que sugería la culpabilidad del acusado procedente de una fuente desconocida´. Sin embargo, la Corte señaló 'la excepción sería el caso en el que el acusado abra la puerta al sugerir falsamente y de forma clara que un oficial de policía actuó de forma arbitraria o con un motivo equivocado' en cuyo caso, 'se puede permitir al oficial despejar esa falsa impresión, a pesar del 'prejuicio que el acusado podría sufrir'.

Aquí, la implicancia del caso Branch no es que el acusado abra la puerta sugiriendo al jurado que la inclusión de su foto en la rueda fue producto de la mala fe, sino más bien que la defensa puede indagar sobre la razón de la identificación del acusado como sospechoso. El descubrimiento [de la FRT] es relevante para la capacidad del acusado de abrir la puerta y convencer al jurado de que la FRT no es fiable e identificó al sospechoso equivocado.

La fiscalía reconoce su obligación de entregar pruebas que permitan excluir la culpabilidad, pero argumenta que la naturaleza exculpatoria de las pruebas solicitadas aquí es ´puramente especulativa´ y es meramente de ´exculpación potencial´. Ya hemos explicado anteriormente, en el contexto de un argumento similar:

El argumento de la fiscalía [la naturaleza de exculpación de la declaración de un testigo era especulativa] asume la verdad de su conclusión y no la explica. Se deja a la defensa especular porque el juez no exigió a la fiscalía que presentara el documento para que sea inspeccionado y que el acusado y su defensa puedan conocer su contenido y determinar su relevancia y materialidad. Puede ser, como sugiere el Estado, irrelevante e inmaterial. Sin embargo, puede ser, como sugiere la defensa, altamente relevante y material e incluso exculpatorio [...]. [Estado ex rel. L.E.W., 239 N.J. Super. 65, 76 (App. Div.), certif. denied, 122 N.J. 144 (1990)].

Aquí, los elementos buscados por la defensa tienen un vínculo directo con la prueba de la fiabilidad de la FRT y tienen que ver con la culpabilidad o inocencia del acusado. Dada la novedad de la FRT, nadie, incluidos nosotros, puede concluir razonablemente sin el descubrimiento [*discovery*] [de la FRT] si la prueba es exculpatoria o ´simplemente una prueba potencialmente útil´. […]. Por estas razones el descubrimiento [*discovery*] de la información debe realizarse.

[A]quí la defensa del acusado ha demostrado una ´necesidad particularizada de descubrimiento [*discovery*]´. […]. Ha presentado una lista de los elementos específicos solicitados, con la ayuda de un experto, que no es ni amplia, ni excesivamente onerosa, ni desvinculada de las pruebas necesarias para establecer una defensa. Como dijo el entonces juez Fasciale en [Sate v. Pickett], A medida que prolifera la tecnología, también lo hace su uso en los procesos penales. Los tribunales deben esforzarse por comprender la nueva tecnología… y permitir a la defensa una oportunidad significativa para examinarla. Sin examinar el código fuente de su software —un conjunto de instrucciones hechas por el hombre que pueden contener errores, fallos y defectos— en el contexto de un sistema acusatorio, no se podría llegar a la conclusión realista de que implementa adecuadamente la ciencia subyacente. En consecuencia, es imperativo permitir un examen significativo del código fuente, que obliga al análisis crítico independiente necesario para que un juez haga una determinación de umbral en cuanto a la fiabilidad en una audiencia […].

Estamos convencidos de que esto también es aplicable para la FRT.

El acusado debe tener las herramientas para impugnar el caso del Estado y sembrar la duda razonable. Por estas razones, revocamos y devolvemos el caso para que se dicte una orden que ordene al Estado proporcionar los once elementos de prueba restantes solicitados por la defensa. Naturalmente, el juez de la moción puede dictar cualquier orden de protección apropiada, ordenar la revisión a puerta cerrada de los materiales recibidos del Estado, y celebrar una audiencia 'Daubert' si es necesario".

# 3. DOCUMENTOS DE INTERÉS

## 3.1. DATYSOC. LABORATORIO DE DATOS Y SOCIEDAD. "FUERA DE CONTROL: USO POLICIAL DEL RECONOCIMIENTO FACIAL AUTOMATIZADO EN URUGUAY. 4/3/2022

Este informe busca aportar elementos para el debate sobre el uso policial del reconocimiento facial automatizado (RFA), explicando aspectos básicos sobre el funcionamiento de esta tecnología y el estado actual de su regulación e implementación en Uruguay. Este documento fue elaborado como respuesta a la ley de presupuesto aprobada por el parlamento uruguayo en 2020 que contenía dos artículos que otorgaban potestad al Ministerio del Interior de ese país a tomar de la base de datos de identificación de la Dirección Nacional de Identificación Civil la fotografía tanto de los documentos de identidad como de los pasaportes para alimentar un sistema de reconocimiento artificial automatizado con fines de seguridad pública.

## 3.2. COMISIÓN NACIONAL DE INFORMÁTICA Y DE LAS LIBERTADES DE FRANCIA. DECISIÓN DEL COMITÉ RESTRINGIDO N.º SAN—2022—019 CONCERNIENTE A CLEARVIEW AI. 17/10/2022

La compañía "Clearview AI", establecida en los Estados Unidos y creada en el año 2017, desarrolló un software basado en el reconocimiento facial que le permitía obtener información a partir de fotografías subidas a sitios gratuitos de internet y construir una base de datos y un motor de búsqueda que luego era comercializado. El software creaba una "plantilla facial" de las personas que aparecían en las imágenes y las guardaba en una base de datos. Luego, en el motor de búsqueda creado por la compañía, se podía buscar a una persona utilizando una fotografía, pues se comparaba su "plantilla facial" con las que contenía la base de datos. Un Comité reducido de la *Commission nationale de l'Informatique et des Libertés* (CNIL, la autoridad francesa de protección de datos) le impuso a la compañía una multa de 20 millones de euros y emitió una orden judicial para que deje de recolectar datos sin una justificación legal de personas que se encuentren en territorio francés y para que borre todos los datos personales de los individuos, en especial de aquellos que presentaron su denuncia.

## 3.3. TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH). GUÍA DE JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS SOBRE PROTECCIÓN DE DATOS PERSONAL. 31/8/2022

Se informan las sentencias y resoluciones fundamentales dictadas por el Tribunal Europeo de Derechos Humanos (TEH) en materia de protección de datos. En esta guía se sostiene que el proceso tecnológico ha dado lugar a un salto cuántico en la vigilancia, la interceptación de las comunicaciones y las conservaciones de datos, lo que su a vez plantea importantes retos para la protección de datos personales.

## 3.4. ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS (ACNUDH) "EL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL". 4/8/2022

El Alto Comisionado de las Naciones Unidas para los Derechos Humanos elaboró un informe temático sobre el impacto de las tecnologías de vigilancia electrónica en la protección de la privacidad. El documento analizaba los riesgos que conllevaban las medidas de hackeo y vigilancia sistemática empleadas por los Estados en el disfrute de los derechos fundamentales. Luego, presentaba lineamientos para garantizar que las medidas de seguridad fueran respetuosas del derecho a la vida privada y familiar.

## 3.5. CONSEJO EUROPEO DE PROTECCIÓN DE DATOS. DIRECTRICES 05/2022 PARA EL USO DE TECNOLOGÍAS DE RECONOCIMIENTO FACIAL. 12/5/2022

En este informe se analiza la implementación la tecnología de reconocimiento facial, así como también las estrategias y el uso de este sistema de inteligencia artificial por parte de los ciudadanos y las organizaciones. Asimismo, se evalúa el impacto de la protección de datos, el uso de la tecnología de reconocimiento facial y la privacidad de las personas.

## 3.6. ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS (ACNUDH) "EL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL". A/HRC/48/31. 13/9/2021

En este informe se analiza cómo el uso generalizado de la inteligencia artificial por parte de los Estados y las empresas, en particular en la elaboración de perfiles, la adopción automatizada de decisiones y las tecnologías de aprendizaje automático, afecta al disfrute del derecho a la privacidad y los derechos conexos. Se examinan varios enfoques para abordar los desafíos que se plantean y se formula un conjunto de recomendaciones para los Estados y las empresas en relación con el diseño y la aplicación de salvaguardias con el objetivo de prevenir y reducir al mínimo los resultados negativos y facilitar el pleno disfrute de los beneficios que puede proporcionar la inteligencia artificial.

## 3.7. PARLAMENTO EUROPEO DE DERECHOS HUMANOS. "ENMIENDAS AL REGLAMENTO DE LA LEY DE INTELIGENCIA ARTIFICIAL (2021)". 14/6/2023

La Ley de IA se creó por dos motivos principales: sincronizar las normas de regulación de la tecnología de IA en todos los Estados miembros de la UE y ofrecer una definición más clara de lo que es realmente la IA. El marco normativo clasifica una amplia gama de aplicaciones por diferentes niveles de riesgo: riesgo inaceptable, alto riesgo, riesgo limitado y riesgo mínimo o nulo. Entre los modelos de riesgo "inaceptable" se incluye a) la manipulación cognitiva del comportamiento de personas o grupos vulnerables específicos: juguetes activados por voz que fomentan comportamientos peligrosos en los niños; b) la puntuación social: clasificación de personas en función de su comportamiento, estatus socioeconómicos o características

personales; y c) los sistemas de identificación biométrica en tiempo real y a distancia, como el reconocimiento facial, aunque incluye algunas excepciones a esta clasificación. Así, las fuerzas de seguridad solo están exentas de restricciones cuando se persigan delitos graves y haya una autorización judicial previa. Este documento que busca frenar los excesos de la Inteligencia Artificial aún debe ser negociado entre el Parlamento Europeo y los Estados miembros.

## 3.8. ALGORITHMIC JUSTICE LEAGUE. TECNOLOGÍAS DE RECONOCIMIENTO FACIAL: INTRODUCCIÓN. 29/5/2020

Este manual está pensado para acompañar al libro blanco: "Facial Recognition Technologies in the Wild: A call for a Federal Office", como documento de apoyo. El documento introductorio presenta los antecedentes de las tecnologías de reconocimiento facial (FRT, siglas en inglés) y proporciona un contexto importante para el material del documento principal del libro blanco. Además, el manual está escrito para un público no técnico con la finalidad de aumentar la comprensión de la terminología, las aplicaciones y las dificultades de evaluar este complejo conjunto de tecnologías. En síntesis, el documento es un tutorial básico.