DIPUTADOS
ARGENTINA

PROYECTO DE LEY

PROYECTO DE LEY SOBRE EL USO DE TECNOLOGÍAS DE RECONOCIMIENTO FACIAL

El Senado y la Honorable Cámara de Diputados de la Nación, reunidos en Congreso, sancionan con fuerza de ley:

TÍTULO I: DISPOSICIONES GENERALES

Artículo 1. Objeto de la Ley. La presente ley tiene por objeto establecer los principios y garantías fundamentales para el desarrollo, implementación, uso y gestión de las tecnologías de reconocimiento facial en el territorio nacional, con el fin de proteger los derechos fundamentales de las personas.

Artículo 2. Definiciones. A los efectos de esta ley, se entenderá por:

a) Reconocimiento facial: Tecnología que permite la identificación o verificación automática de la identidad de una persona mediante el análisis de sus rasgos faciales distintivos.

b) Datos biométricos faciales: Información relativa a las características físicas del rostro de una persona que permiten su identificación única.

c) Sistema de reconocimiento facial (SRF): Conjunto de hardware y software que permite la captura, procesamiento, almacenamiento y comparación de datos biométricos faciales.

d) Evaluación de impacto: Proceso sistemático de evaluación de los posibles efectos adversos del uso de tecnologías de reconocimiento facial sobre los derechos fundamentales de las personas.

e) Sesgos algorítmicos: Errores sistemáticos, configuraciones arbitrarias o discriminatorias en el diseño, entrenamiento o funcionamiento de los sistemas de reconocimiento facial que pudieren conducir a discriminación, identificaciones incorrectas de ciertos grupos demográficos, o tratamiento diferenciado injustificado basado en características protegidas como raza, género, edad, origen étnico, religión u orientación sexual.

f) Transparencia algorítmica: Obligación de proporcionar información comprensible sobre el funcionamiento, criterios de decisión, datos de entrenamiento y parámetros de configuración de los sistemas de reconocimiento facial, de manera que permitan su evaluación, auditoría y supervisión efectiva.

g) Auditoría algorítmica: Proceso de evaluación técnica independiente del funcionamiento, precisión, sesgos y conformidad normativa de los sistemas de reconocimiento facial.

Artículo 3. Ámbito de aplicación. Esta ley se aplicará a:

a) Las entidades públicas nacionales que implementen o utilicen tecnologías de reconocimiento facial para fines de seguridad ciudadana, prevención de delitos e investigación judicial.

b) Las entidades privadas que desarrollen y/o comercialicen tecnologías de reconocimiento facial para entidades públicas en el marco de los fines establecidos en esta ley.

c) Las provincias y la Ciudad Autónoma de Buenos Aires, en caso de adhesión.

Artículo 4. Principios rectores**.** La implementación y uso de tecnologías de reconocimiento facial deberá regirse por los siguientes principios:

a) Legalidad: Todo uso de tecnologías de reconocimiento facial deberá estar autorizado por ley.

b) Proporcionalidad: Su uso deberá ser proporcional a los fines perseguidos.

c) Necesidad: Su implementación deberá ser estrictamente necesaria para lograr los objetivos legítimos.

d) Transparencia: Las personas tendrán derecho a ser informadas sobre la existencia y finalidad de los sistemas.

e) Transparencia algorítmica: Los sistemas deberán ser auditables y comprensibles en su funcionamiento.

f) No discriminación: Los sistemas no deberán producir resultados discriminatorios.

g) Responsabilidad: Las entidades implementadoras serán responsables del adecuado funcionamiento de los sistemas.

h) Supervisión independiente: Se garantizará la supervisión por órganos de control independientes.

TÍTULO II: GARANTÍAS FUNDAMENTALES

Artículo 5. Autorización y condiciones previas. La implementación de sistemas de reconocimiento facial requerirá la autorización previa de la autoridad de aplicación y deberá estar precedida por una Evaluación de Impacto en Derechos Humanos y Protección de Datos Personales. La autoridad de aplicación será la encargada de establecer los contenidos mínimos de dichas evaluaciones, así como los procedimientos para

su presentación y aprobación.

Artículo 6. Limitación de propósito. Los sistemas de reconocimiento facial sólo podrán implementarse para los siguientes fines específicos:

a) Prevención e investigación de aquellos delitos tipificados en los Títulos I, III, V, VI, VII, VIII, IX y X del Libro II del Código Penal.

b) Identificación de personas con órdenes de detención pendientes.

c) Búsqueda de personas desaparecidas.

d) Seguridad en infraestructuras críticas, previa justificación de necesidad por parte de la entidad pública nacional, validada por la autoridad de aplicación.

1. Queda prohibido el uso de sistemas de reconocimiento facial para cualquier otro fin de los previstos en el inciso anterior del presente artículo, siendo además pasible de sanción por parte de la Autoridad de Aplicación la detección del uso para los siguientes fines:

   a) Vigilancia masiva e indiscriminada.

   b) Seguimiento rutinario de personas que no son sospechosas de delitos.

   c) Creación de perfiles basados en características protegidas.

Artículo 7. Intervención humana. Los sistemas de reconocimiento facial no podrán tomar decisiones automatizadas sin intervención humana cuando estas afecten los derechos de las personas, y toda identificación que se realice mediante estos sistemas deberá ser verificada por un operador humano capacitado antes de tomar cualquier acción.

Artículo 8. Control judicial. El uso de tecnologías de reconocimiento facial con fines de investigación criminal requerirá autorización judicial previa, salvo en casos de urgencia debidamente justificados, en los cuales deberá obtenerse convalidación judicial dentro de las 24 horas.

Artículo 9. Transparencia algorítmica y auditabilidad. Los sistemas de reconocimiento facial implementados conforme a esta ley deberán cumplir con los siguientes requisitos de transparencia algorítmica:

a) Documentación técnica completa: Los proveedores deberán entregar documentación detallada sobre la arquitectura del sistema, algoritmos utilizados, datos de entrenamiento, parámetros de configuración y métricas de rendimiento.

b) Acceso para auditoría: Los sistemas deberán permitir el acceso completo para auditorías técnicas independientes, sin que pueda invocarse secreto comercial, industrial o cualquier otra reserva para impedir la evaluación de su funcionamiento.

c) Código auditable: Cuando sea técnicamente factible, el código fuente de los algoritmos críticos deberá estar disponible para revisión por parte de auditores autorizados.

d) Explicabilidad de decisione**s**: Los sistemas deberán proporcionar información comprensible sobre los criterios utilizados para cada identificación o decisión.

2. Los proveedores de tecnología no podrán invocar secreto comercial, industrial o derechos de propiedad intelectual para:

a) Impedir auditorías algorítmicas ordenadas por la autoridad de aplicación.

b) Ocultar información sobre sesgos, errores o limitaciones del sistema.

c) Restringir el acceso a datos necesarios para evaluar el cumplimiento de esta ley.

3. La autoridad de aplicación establecerá protocolos de confidencialidad que protejan la información comercial legítima sin comprometer la transparencia algorítmica requerida.

Artículo 10. Trazabilidad y registro de operaciones.Los sistemas de reconocimiento facial deberán mantener registros completos, inmutables y auditables de todas las operaciones realizadas, incluyendo:

a) Identificación del operador autorizado.

b) Fecha y hora exacta de cada acceso y consulta.

c) Propósito específico de cada operación.

d) Resultados obtenidos y nivel de confianza.

e) Decisiones adoptadas tras la intervención humana obligatoria.

f) Autorizaciones judiciales o administrativas que respaldan cada operación.

2. Los registros deberán conservarse por un período mínimo de cinco (5) años y estar disponibles para auditorías y controles judiciales.

3. La autoridad de aplicación establecerá estándares técnicos para garantizar la integridad, autenticidad y no repudio de los registros.

TÍTULO III: PROTECCIÓN DE DATOS Y DERECHOS

Artículo 11. Tratamiento de datos biométricos**.**Los datos biométricos faciales serán considerados datos sensibles conforme a la legislación de protección de datos personales.Queda prohibida la creación de bases de datos biométricas faciales generales de toda la población.

Artículo 12. Derechos de los afectadosLas personas cuyos datos sean tratados mediante sistemas de reconocimiento facial tendrán los siguientes derechos:

a) Derecho a la información sobre la existencia de sistemas de reconocimiento facial.

b) Derecho de acceso a sus datos biométricos registrados.

c) Derecho de rectificación y supresión.

d) Derecho a impugnar decisiones basadas en el reconocimiento facial.

e) Derecho a indemnización por daños causados por identificaciones erróneas o usos indebidos.

f) Derecho a conocer la lógica y criterios de funcionamiento del sistema que los afecte.

La autoridad de aplicación establecerá procedimientos expeditos y gratuitos para el ejercicio de los derechos reconocidos en el artículo anterior.

TÍTULO IV: MECANISMOS DE SUPERVISIÓN Y CONTROL

Artículo 13. Autoridad de aplicación. La Agencia de Acceso a la Información Pública, o el organismo que en el futuro la reemplace, será la autoridad de aplicación de la presente ley y tendrá las siguientes funciones, de modo enunciativo más no taxativo:

a) Autorizar la implementación de sistemas de reconocimiento facial.

b) Establecer estándares técnicos mínimos.

c) Aprobar las evaluaciones de impacto.

d) Realizar auditorías periódicas.

e) Investigar denuncias sobre posibles infracciones.

f) Imponer sanciones en caso de incumplimiento.

g) Emitir recomendaciones y directrices.

h) Promover la investigación y mejora de estas tecnologías.

i) Presentar un informe anual al Congreso de la Nación.

j) Establecer y supervisar el cumplimiento de los estándares de transparencia algorítmica.

k) Autorizar y supervisar auditorías algorítmicas independientes.

Artículo 14. Auditorías algorítmicas.Los sistemas de reconocimiento facial estarán sujetos a auditorías algorítmicas obligatorias antes de su puesta en funcionamiento y periódicamente durante su operación.Las mismas deberán evaluar:

a) Precisión y confiabilidad del sistema.

b) Existencia de sesgos algorítmicos.

c) Cumplimiento de los principios de no discriminación.

d) Adecuación a los fines autorizados.

e) Seguridad y protección de datos.

f) Transparencia y explicabilidad de las decisiones.

3. Las auditorías serán realizadas por organismos técnicos independientes acreditados por la autoridad de aplicación.

4. Los resultados de las auditorías serán públicos, salvaguardando la información que pueda comprometer la seguridad nacional o investigaciones en curso.

Artículo 15. Participación ciudadana**.**La autoridad de aplicación establecerá en la reglamentación mecanismos de participación ciudadana, que incluirán consultas públicas y la conformación de un órgano consultivo multisectorial.

TÍTULO V: INFRACCIONES Y SANCIONES

Artículo 16. Infracciones y Sanciones. La Autoridad de Aplicación se encuentra plenamente facultada para la aplicación de infracciones y sanciones, conforme lo establezca en la reglamentación correspondiente.

A tal efecto, la Autoridad de Aplicación establecerá un procedimiento sancionador que garantice el debido proceso, la defensa y los recursos administrativos y judiciales correspondientes, así como también los mecanismos de seguimiento necesarios para garantizar la efectiva implementación de las medidas correctivas impuestas.

La Autoridad de Aplicación deberá publicar los actos sancionatorios en su sitio web y en el Boletín Oficial de la República Argentina, hallándose facultada para notificar a la Comisión Bicameral de

Fiscalización de los Organismos y Actividades de Inteligencia del Congreso de la Nación, en los casos que la reglamentación así lo determine en virtud de la materia y la gravedad de la infracción.

Las infracciones relacionadas con la falta de transparencia algorítmica, el impedimento de auditorías o la invocación indebida de secreto comercial serán consideradas faltas graves.

TÍTULO VI: DISPOSICIONES FINALES

Artículo 17. Adhesión de las provincias y de la Ciudad Autónoma de Buenos Aires. Se invita a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir a la presente ley.

Artículo 18. Reglamentación**.**La Autoridad de Aplicación reglamentará la presente ley dentro de los ciento ochenta (180) días corridos a partir de su publicación en el Boletín Oficial.

Artículo 19. Adaptación de sistemas existentes**.**Los sistemas de reconocimiento facial que se encontraren operativos a la entrada en vigor de esta ley contarán con un plazo de doce (12) meses para adaptarse a sus requisitos.

Artículo 20. Entrada en vigor.La presente ley entrará en vigor a los noventa (90) días de su publicación en el Boletín Oficial.

Artículo 21. De forma. Comuníquese al Poder Ejecutivo Nacional.

Autor:

YEZA, Martín

Co-Firmantes

CAPOZZI, Sergio Eduardo
RODRÍGUEZ MACHADO, Laura
SÁNCHEZ WRBA, Javier
ARDOHAIN, Martín
BACHEY, Karina Ethel
FIGUEROA CASAS, Germana
DE SENSI, María Florencia
BALLEJOS, Nancy
BIANCHETTI, Emanuel
TORTORIELLO, Anibal

FERNÁNDEZ MOLERO, Daiana
AVICO, Belén
LOSPENNATO, Silvia

FUNDAMENTOS

Sr. Presidente:

El presente proyecto tiene por objeto la regulación del desarrollo, implementación, uso y gestión de las tecnologías de reconocimiento facial en la República Argentina, a través del establecimiento de principios y garantías fundamentales en pos de la protección de los derechos fundamentales de las personas. Ello, por los motivos que a continuación procedemos a esgrimir.

1. Contexto y necesidad regulatoria

En los últimos años, hemos sido testigos de un avance acelerado de las tecnologías de reconocimiento facial como herramientas para la seguridad ciudadana y la prevención del delito. Sin embargo, estas tecnologías han sido implementadas de forma fragmentada en diversas jurisdicciones del país, sin un marco normativo integral que garantice tanto su eficacia como el respeto a los derechos fundamentales de las personas.

La ausencia de una legislación específica en esta materia ha generado una situación de incertidumbre jurídica que afecta tanto a las instituciones públicas que implementan estas tecnologías como a los ciudadanos cuyos datos biométricos son procesados. Esta laguna legal constituye un riesgo para la privacidad y los derechos digitales de los argentinos, al tiempo que limita el potencial de estas herramientas para contribuir efectivamente a la seguridad pública.

2. Tendencias internacionales y posicionamiento de Argentina

Nuestro país no puede mantenerse ajeno a la tendencia internacional de regular estas tecnologías. Tanto en la Unión Europea -a través de su Reglamento de Inteligencia Artificial- como en América Latina -con países como Brasil y Chile- se ha propiciado avanzar en marcos regulatorios específicos para el uso de sistemas de reconocimiento facial en espacios públicos.

En este sentido, en respeto a su tradición de liderazgo regional en materia de derechos digitales, es preciso que Argentina dé un paso decisivo en este sentido.

2.1 Modelos internacionales de referencia en implementación de reconocimiento facial

En la elaboración de este proyecto de ley, hemos analizado diversas experiencias internacionales que representan paradigmas de innovación en la implementación responsable de tecnologías de reconocimiento facial:

Estonia

Estonia, reconocido líder mundial en gobierno digital, ha implementado un enfoque integrado de reconocimiento facial dentro de su ecosistema de identidad digital (e-ID). El modelo estonio destaca por:

- La integración del reconocimiento facial con la infraestructura X-Road, que permite la interoperabilidad entre distintos sistemas gubernamentales sin comprometer la privacidad.
- La implementación del principio de "una sola vez", evitando que los ciudadanos deban proporcionar repetidamente sus datos biométricos.
- El establecimiento de controles democráticos robustos, incluyendo comités parlamentarios de supervisión y evaluaciones independientes periódicas.

Corea del Sur

Corea del Sur ha desarrollado un marco regulatorio avanzado para el reconocimiento facial que combina innovación tecnológica con protecciones sólidas a la privacidad:

- Creación del "K-Identification System", que establece distintos niveles de verificación biométrica según la sensibilidad del servicio.
- Implementación de protocolos avanzados de seguridad y trazabilidad en los sistemas gubernamentales de reconocimiento facial.
- Separación estricta entre datos biométricos utilizados para servicios públicos y para investigación criminal.
- Establecimiento de la "K-Data Protection Commission", un organismo independiente con facultades de supervisión y sanción.

Reino Unido

El Reino Unido ha desarrollado un enfoque matizado que equilibra la seguridad pública con la protección de derechos fundamentales:

- Implementación de un "Código de Práctica para el Reconocimiento Facial" que establece estándares obligatorios para todas las fuerzas policiales.
- Creación del "Biometrics and Surveillance Camera Commissioner", un organismo independiente que supervisa el uso de tecnologías de reconocimiento facial.
- Establecimiento de procedimientos de "Autorización de Vigilancia" con controles judiciales para el uso de reconocimiento facial en tiempo real.
- Desarrollo de un marco de "Evaluación de Necesidad y Proporcionalidad" que debe completarse antes de cada despliegue.

Estos modelos internacionales ofrecen lecciones valiosas para Argentina, particularmente en lo referente a la implementación de sistemas robustos de transparencia algorítmica, organismos independientes de supervisión, y el establecimiento de un marco legal que equilibre seguridad y privacidad.

3. Fundamentos del proyecto

El presente proyecto responde a una necesidad social y jurídica imperante, proporcionando un marco normativo equilibrado que permita aprovechar las ventajas de estas tecnologías para la seguridad ciudadana, sin comprometer los derechos fundamentales consagrados en nuestra Constitución Nacional y

en los tratados internacionales de derechos humanos que gozan de jerarquía constitucional conforme al artículo 75, inciso 22 de nuestra Carta Magna.

La iniciativa se sustenta en principios fundamentales como la legalidad, proporcionalidad, necesidad, transparencia, transparencia algorítmica, no discriminación y responsabilidad. Estos principios, desarrollados por nuestra jurisprudencia constitucional y por organismos internacionales de derechos humanos, constituyen el fundamento axiológico del proyecto.

Asimismo, el texto propuesto reconoce la estructura federal de nuestro país, respetando las autonomías provinciales y estableciendo mecanismos de coordinación, con el objetivo de armonizar criterios y estándares en todo el territorio nacional.

4. Aspectos destacados de la propuesta

Entre los aspectos más destacados de la propuesta, cabe mencionar:

- La creación de un sistema de autorizaciones previas y evaluaciones de impacto obligatorias, que garantiza que estas tecnologías solo sean implementadas cuando sean estrictamente necesarias y proporcionales.
- El establecimiento de límites claros a los propósitos para los cuales pueden utilizarse estas tecnologías, prohibiendo expresamente la vigilancia masiva e indiscriminada y el seguimiento rutinario de personas no sospechosas.
- La exigencia de requisitos técnicos rigurosos que aseguren la precisión de los sistemas y la ausencia de sesgos discriminatorios.
- La garantía de intervención humana en todas las decisiones basadas en reconocimiento facial que puedan afectar los derechos de las personas.
- El reconocimiento de derechos específicos para los ciudadanos afectados, como el derecho a la información, acceso, rectificación, supresión e impugnación, incluyendo el derecho a conocer la lógica y criterios de funcionamiento del sistema.
- El establecimiento de un control judicial previo para el uso de estas tecnologías en investigaciones criminales.
- La designación de la Agencia de Acceso a la Información Pública como autoridad de aplicación.
- La implementación de un sistema de auditorías algorítmicas obligatorias y mecanismos de transparencia activa.

4.1 Transparencia algorítmica como principio fundamental

Una innovación destacada del presente proyecto es la incorporación de estándares avanzados de transparencia algorítmica que garantizan la auditabilidad, comprensibilidad y supervisión efectiva de los sistemas de reconocimiento facial. En particular, se establece un marco normativo que prescribe:

Documentación técnica completa

Los proveedores deberán entregar documentación detallada sobre la arquitectura del sistema, algoritmos utilizados, datos de entrenamiento, parámetros de configuración y métricas de rendimiento. Esta exigencia permite:

- **Evaluación técnica rigurosa**: Las autoridades competentes podrán evaluar la idoneidad y seguridad de los sistemas antes de su implementación.
- **Identificación de limitaciones**: La documentación completa facilita la detección temprana de posibles sesgos o fallas en el diseño.
- **Mejora continua**: La transparencia en la documentación técnica permite la evolución y perfeccionamiento de los sistemas.

Prohibición del secreto comercial como impedimento para auditorías

El proyecto establece expresamente que los proveedores no podrán invocar secreto comercial, industrial o derechos de propiedad intelectual para:

- Impedir auditorías algorítmicas ordenadas por la autoridad de aplicación.
- Ocultar información sobre sesgos, errores o limitaciones del sistema.
- Restringir el acceso a datos necesarios para evaluar el cumplimiento de la ley.

Esta disposición representa un avance significativo hacia la **democratización del control tecnológico**, garantizando que el interés público prevalezca sobre consideraciones comerciales cuando se trata de tecnologías que pueden afectar derechos fundamentales.

Auditorías algorítmicas obligatorias

Se establece un sistema comprensivo de auditorías que evaluará:

- Precisión y confiabilidad del sistema
- Existencia de sesgos algorítmicos
- Cumplimiento de los principios de no discriminación
- Adecuación a los fines autorizados
- Seguridad y protección de datos
- Transparencia y explicabilidad de las decisiones

Las auditorías serán realizadas por organismos técnicos independientes acreditados por la autoridad de aplicación, garantizando así la objetividad y rigor técnico de las evaluaciones.

Trazabilidad y registro de operaciones

El proyecto prescribe el mantenimiento de registros completos, inmutables y auditables de todas las operaciones realizadas, incluyendo identificación del operador, fecha y hora exacta, propósito específico, resultados obtenidos y decisiones adoptadas. Esta trazabilidad permite:

- **Accountability efectivo**: Cada acción queda registrada de manera verificable.

- **Evidencia forense robusta**: Los registros constituyen evidencia digital sólida para procesos judiciales.
- **Prevención de abusos**: La trazabilidad disuade el uso indebido de los sistemas.

La implementación de estos estándares de transparencia algorítmica posiciona a Argentina a la vanguardia mundial en la regulación de sistemas de reconocimiento facial, estableciendo un paradigma que equilibra la innovación tecnológica con la protección robusta de derechos fundamentales.

5. Antecedentes de implementación en Argentina

En los últimos años, diversas jurisdicciones argentinas han implementado sistemas de reconocimiento facial:

- El Sistema de Reconocimiento Facial de Prófugos (SRFP) de la Ciudad Autónoma de Buenos Aires, implementado en 2019, suspendido por decisión judicial en 2022 por no contar con las garantías suficientes para la protección de datos personales y derechos fundamentales.
- Sistemas similares implementados en provincias como Mendoza, Salta y Córdoba, con distintos niveles de control y transparencia.
- Proyectos piloto en municipios como Tigre, Vicente López y San Isidro en la Provincia de Buenos Aires.

Estas implementaciones se han realizado sin un marco regulatorio nacional específico, generando un mosaico de normativas locales con distintos niveles de protección de derechos y garantías procedimentales.

6. Marco Constitucional y Legal Argentino

El presente proyecto de ley se fundamenta en el siguiente marco normativo:

6.1. Base constitucional

Es importante mencionar que este proyecto se enmarca también en diversas cláusulas constitucionales. Por un lado el artículo 18 de la Constitución Nacional garantiza la inviolabilidad del domicilio, la correspondencia epistolar y los papeles privados, estableciendo un principio de privacidad que se extiende a los datos biométricos. Asimismo, el artículo 19 consagra el principio de reserva y libertad individual, protegiendo las acciones privadas de los hombres que no ofendan al orden público. Por su parte, el artículo 43 establece la acción de hábeas data, otorgando rango constitucional a la protección de datos personales.

Del mismo modo, los tratados internacionales de derechos humanos con jerarquía constitucional, conforme al artículo 75 inciso 22 de la Constitución Nacional, particularmente el Pacto Internacional de Derechos Civiles y Políticos (artículo 17) y la Convención Americana sobre Derechos Humanos (artículo 11), protegen el derecho a la privacidad y a la honra.

6.2. Marco legal vigente

- **Ley 25.326 de Protección de Datos Personales**: Establece los principios generales de protección de datos personales, incluyendo los datos sensibles, categoría donde se encuadran los datos biométricos.
- **Ley 27.078 Argentina Digital**: Establece principios sobre el desarrollo de tecnologías de información y comunicación.
- **Ley 27.275 de Acceso a la Información Pública**: Establece principios de transparencia aplicables a la implementación de tecnologías por parte del Estado.
- **Código Procesal Penal de la Nación y códigos procesales provinciales**: Regulan las condiciones para la obtención de pruebas y medidas de investigación que pueden incluir el uso de tecnologías de reconocimiento facial.
- **Resolución 4/2019 de la Agencia de Acceso a la Información Pública**: Aborda específicamente el tratamiento de datos biométricos, aunque de forma general.

6.3. Fallos judiciales relevantes

- **"Asociación Civil por la Igualdad y la Justicia c/ GCBA s/ Amparo" (2022)**: Donde el Juzgado en lo Contencioso Administrativo y Tributario N° 2 de la Ciudad de Buenos Aires suspendió el Sistema de Reconocimiento Facial de Prófugos, señalando deficiencias en materia de protección de datos personales y garantías procedimentales.

- **"Observatorio de Derecho Informático Argentino O.D.I.A. y otros c/ GCBA s/ amparo - otros" (2023)**: Donde se suspendió el uso de la tecnología de Reconocimiento Facial de Prófugos (SRFP) debido a las consecuencias que acarreaba su implementación prematura y en condiciones precarias de respeto por los derechos y garantías de las personas.

Con referencia a la sentencia "Observatorio de Derecho Informático Argentino O.D.I.A. y otros c/ GCBA s/ amparo - otros", que suspendió el uso del SRFP en CABA, la suspensión se fundamentó en las consecuencias de su implementación prematura y en condiciones precarias de respeto por los derechos y garantías de las personas.

Los principales problemas y deficiencias identificados en la sentencia respecto a la implementación del SRFP fueron:

- La ausencia de una Evaluación de Impacto en la Privacidad (EIP) o en la Protección de Datos Personales (EIPD) antes de la implementación. La sentencia la consideró una herramienta fundamental.
- La falta de constitución o el debido funcionamiento de los organismos de control previstos en la normativa, como la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia en el ámbito de la Legislatura de la Ciudad y la Defensoría del Pueblo. Se señaló que estos organismos no pudieron ejercer sus funciones de fiscalización.
- La existencia de fallas en la base de datos CONARC utilizada por el sistema, lo que podía generar "falsos positivos" y, consecuentemente, detenciones o demoras erróneas.

- La exclusión de la participación ciudadana en el debate y la implementación del sistema.
- Preocupaciones sobre la proporcionalidad, necesidad y el riesgo de convertirse en un sistema de vigilancia masiva.

Es importante destacar que la sentencia no declaró la inconstitucionalidad del SRFP en sí mismo, sino de su implementación sin los resguardos adecuados. La reactivación del SRFP quedó supeditada a la constitución y el debido funcionamiento de los órganos de control, así como a la realización de pruebas sobre el software para determinar si tenía un impacto diferenciado o sesgos y a la publicidad e información en los Foros de Seguridad Pública (FOSEP).

7. Relación del proyecto con los casos judiciales

El proyecto de ley sobre el uso de tecnologías de reconocimiento facial propuesto está diseñado para establecer un marco normativo integral que aborde precisamente este tipo de preocupaciones a nivel nacional. El proyecto invita a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir a sus disposiciones.

Si la Ciudad de Buenos Aires adhiriera a este proyecto de ley, la implementación y el uso de tecnologías de reconocimiento facial como el SRFP estarían sujetos a requisitos y salvaguardas que buscan prevenir las deficiencias identificadas en la sentencia judicial:

- **Evaluación de impacto obligatoria**: El proyecto de ley exige la realización de una Evaluación de Impacto en Derechos Humanos y Protección de Datos Personales previo a la implementación de cualquier sistema, la cual debe incluir un análisis de riesgos, medidas de mitigación y análisis de sesgos. Esta evaluación debe ser revisada y aprobada por la autoridad de aplicación.

- **Supervisión independiente**: Se establece la necesidad de mecanismos de supervisión independiente para garantizar el cumplimiento de la ley. Las jurisdicciones que adhieran pueden coordinar con la autoridad nacional (la Agencia de Acceso a la Información Pública).

- **Limitación de propósitos, necesidad y proporcionalidad**: El proyecto establece que el uso debe ser estrictamente necesario y proporcional a los fines legítimos perseguidos. Define fines específicos y limitados para los que se puede usar la tecnología (ej. identificación de prófugos con orden de detención), y prohíbe expresamente la vigilancia masiva e indiscriminada.

- **No discriminación y sesgos**: El proyecto exige requisitos técnicos rigurosos para asegurar la ausencia de sesgos discriminatorios y establece auditorías algorítmicas obligatorias para detectar y corregir sesgos.

- **Transparencia y derechos ciudadanos**: Se garantiza el derecho de los ciudadanos a ser informados sobre la existencia y finalidad de los sistemas, y se reconocen derechos específicos como acceso, rectificación, supresión e impugnación, incluyendo el derecho a conocer la lógica y criterios de funcionamiento del sistema.

- **Intervención humana**: Se requiere la verificación humana de cualquier identificación realizada por el sistema antes de tomar acciones que afecten derechos. Se prohíben las decisiones automatizadas sin intervención humana.

- **Control judicial**: Para fines de investigación criminal, el uso requeriría autorización judicial previa, con la posibilidad de convalidación judicial en casos de urgencia.

- **Adaptación de sistemas existentes**: Los sistemas ya operativos a la entrada en vigor de la ley tendrían un plazo de 12 meses para adaptarse a los nuevos requisitos.

- **Transparencia algorítmica y trazabilidad**: La implementación de estándares de transparencia algorítmica garantiza que los sistemas sean auditables y comprensibles, mientras que los registros inmutables de todas las operaciones permiten una supervisión exhaustiva y accountability efectivo.

- **Auditorías algorítmicas independientes**: La realización de auditorías técnicas por organismos independientes asegura la evaluación objetiva del funcionamiento, precisión y ausencia de sesgos en los sistemas.

Por lo tanto, la sentencia judicial suspendió el SRFP en CABA por la falta de las garantías que el proyecto de ley busca establecer como condición previa y continua para el uso de tecnologías de reconocimiento facial. Si la Ciudad de Buenos Aires adhiriera a este proyecto de ley (o adoptara una normativa local con salvaguardas equivalentes en coordinación con el marco nacional), la implementación de tales sistemas podría considerarse compatible con las exigencias de protección de derechos señaladas en la sentencia, siempre y cuando se cumplieran todos los requisitos de la ley, incluyendo la evaluación de impacto, el funcionamiento de los controles, la mitigación de sesgos y fallas en las bases de datos, y los mecanismos de transparencia y participación ciudadana. La ley proporciona el marco legal que la sentencia encontró ausente en la implementación inicial del SRFP en CABA.

8. Conclusión

Este proyecto ha sido elaborado tras un exhaustivo análisis y su redacción busca equilibrar la protección de derechos fundamentales con la necesidad de contar con herramientas tecnológicas eficaces para la prevención e investigación del delito.

La incorporación de estándares avanzados de transparencia algorítmica, auditorías independientes y trazabilidad completa de operaciones, siguiendo las mejores prácticas internacionales de países como Estonia, Corea del Sur y Reino Unido, posiciona a Argentina a la vanguardia en la regulación de estas tecnologías, estableciendo un estándar elevado de protección de derechos sin renunciar a los beneficios que estas herramientas pueden aportar a la seguridad pública.

El enfoque tecnológicamente neutro del proyecto permite la flexibilidad necesaria para adaptar las implementaciones a los avances tecnológicos futuros, manteniendo siempre como eje central la protección de los derechos fundamentales y la transparencia en el uso de estas poderosas herramientas.

Estamos convencidos de que esta iniciativa representa un avance significativo hacia un modelo de seguridad ciudadana tecnológicamente avanzado pero respetuoso de los valores democráticos y los derechos humanos consagrados en nuestra Constitución Nacional.

Por todo lo expuesto, es que solicito el acompañamiento de mis pares.

YEZA,MARTÍN
Diputado Nacional por la Provincia de Buenos Aires