PROYECTO DE LEY

EL SENADO Y LA CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA

REUNIDOS EN CONGRESO SANCIONAN CON FUERZA DE LEY:

LEY DE PROTECCIÓN DE DATOS BIOMÉTRICOS

Y REGULACIÓN DEL RECONOCIMIENTO FACIAL

TÍTULO I — DISPOSICIONES GENERALES

ARTÍCULO 1º — *Objeto.*

La presente ley tiene por objeto regular la recolección, almacenamiento, procesamiento, uso y eliminación de datos biométricos, con especial énfasis en los sistemas de reconocimiento facial y otras tecnologías de identificación biométrica, a fin de proteger los derechos fundamentales a la privacidad, la dignidad, la igualdad, la libertad de circulación y la no discriminación de las personas en la República Argentina, y de promover el desarrollo de una industria biométrica nacional responsable, competitiva y soberana.

ARTÍCULO 2º — *Ámbito de aplicación.*

La presente ley se aplica a toda persona humana o jurídica, pública o privada, que recolecte, almacene, procese, utilice o transfiera datos biométricos en territorio argentino o de personas que se encuentren en él.

Quedan exceptuados:

a) Los tratamientos realizados por una persona humana con fines exclusivamente personales o domésticos.

b) Los tratamientos realizados en el marco de investigaciones científicas con datos anonimizados de manera irreversible y aprobados por un comité de ética

acreditado.

ARTÍCULO 3º — *Definiciones.*

A los efectos de la presente ley se entiende por:

a) Dato biométrico: dato personal obtenido a partir de un tratamiento técnico específico, relativo a las características físicas, fisiológicas o conductuales de una persona humana que permita o confirme su identificación única. Incluye, sin limitarse a: imágenes faciales y geometría facial; huellas dactilares y palmares; patrones de iris y retina; patrón de voz; patrones de marcha y postura; geometría de la mano; patrones vasculares; ADN con fines identificatorios; y neurodatos con fines de identificación biométrica.

b) Identificación biométrica: proceso de comparar los datos biométricos de una persona con una base de datos biométricos de múltiples personas para establecer su identidad (comparación uno a muchos).

c) Verificación biométrica: proceso de comparar los datos biométricos de una persona con los datos biométricos previamente registrados de esa misma persona para confirmar su identidad declarada (comparación uno a uno).

d) Reconocimiento facial: tecnología que utiliza características únicas del rostro de una persona para su identificación o verificación, incluyendo la detección de rostros, la extracción de características faciales y la comparación con bases de datos.

e) Identificación biométrica remota: sistema de inteligencia artificial destinado a identificar personas a distancia sin su participación activa, mediante la comparación de datos biométricos capturados con bases de datos de referencia.

f) Identificación biométrica remota en tiempo real: identificación biométrica remota que se produce de forma simultánea o con demora insignificante respecto de la captura de los datos biométricos.

g) Identificación biométrica remota posterior: identificación biométrica remota que se realiza tras la captura y almacenamiento de los datos biométricos, con demora significativa.

h) Categorización biométrica: sistema que clasifica a personas en categorías basadas en sus datos biométricos, tales como género estimado, edad, origen étnico, estado emocional u otras características.

i) Reconocimiento de emociones: sistema que infiere estados emocionales, sentimientos, intenciones o estados psíquicos a partir de datos biométricos, distinguiéndose de la mera detección de expresiones faciales o estados físicos manifiestos.

j) Base de datos biométricos: todo archivo, registro o banco de datos que contenga datos biométricos de múltiples personas.

k) Vigilancia biométrica masiva: uso de sistemas de identificación biométrica remota que, por su escala, continuidad o ubicuidad, permiten el monitoreo sistemático de la población o de segmentos significativos de ella en espacios de acceso público. Se considerará masivo todo sistema que reúna al menos dos de las siguientes características: i) opera de manera no dirigida, es decir, sin objetivo de identificación de una persona determinada o determinable previamente individualizada; ii) captura datos biométricos de manera indiscriminada de todas o la mayoría de las personas que transitan por la zona de cobertura; iii) opera de forma continua o recurrente por períodos superiores a veinticuatro (24) horas; iv) cubre simultáneamente más de un (1) punto de captura o una superficie superior a quinientos (500) metros cuadrados de espacio de acceso público.

l) Espacio de acceso público: todo espacio físico accesible a un número indeterminado de personas, con independencia de la titularidad pública o privada del inmueble.

m) Nivel de riesgo biométrico: clasificación del tratamiento de datos biométricos en función de su impacto potencial sobre los derechos fundamentales. Se establecen tres niveles: i) riesgo bajo: verificación biométrica uno a uno con consentimiento, procesamiento local, sin almacenamiento centralizado; ii) riesgo medio: identificación biométrica uno a muchos en entornos controlados con consentimiento y base de datos limitada a menos de diez mil (10.000) registros; iii) riesgo alto: identificación biométrica remota, bases de datos superiores a diez mil (10.000) registros, tratamiento sin consentimiento en supuestos legales, o cualquier uso con efectos jurídicos directos sobre las personas.

TÍTULO II — PRINCIPIOS Y DERECHOS

ARTÍCULO 4º — *Principios.*

El tratamiento de datos biométricos se regirá por los principios establecidos en la Ley de Protección Integral de Datos Personales y, adicionalmente, por los siguientes principios específicos:

a) Necesidad estricta: los datos biométricos solo podrán ser recolectados y tratados cuando sea estrictamente necesario para la finalidad declarada y no exista un medio menos invasivo para alcanzarla.

b) Irretroactividad del consentimiento: el consentimiento para un fin específico no habilita el uso de los datos biométricos para fines distintos, ni su incorporación a bases de datos no contempladas en el consentimiento original.

c) Temporalidad: los datos biométricos serán eliminados una vez cumplida la finalidad para la cual fueron recolectados, salvo obligación legal de conservación.

d) Prohibición de enriquecimiento: queda prohibida la combinación de datos biométricos con otras fuentes de datos para generar perfiles integrales de la persona sin su consentimiento explícito.

e) Transparencia activa: todo sistema de identificación o verificación biométrica debe ser claramente señalizado e informado a las personas antes de que sus datos sean capturados.

f) Proporcionalidad regulatoria: las obligaciones impuestas por la presente ley se aplicarán de manera escalonada en función del nivel de riesgo biométrico definido en el artículo 3 inciso m), de modo que los tratamientos de riesgo bajo tendrán cargas regulatorias proporcionalmente menores a los de riesgo alto.

ARTÍCULO 5º — *Derechos específicos.*

Además de los derechos consagrados en la Ley de Protección Integral de Datos Personales, toda persona tiene derecho a:

a) Conocer si sus datos biométricos se encuentran almacenados en cualquier base de datos y obtener acceso gratuito a dicha información.

b) Solicitar la eliminación inmediata e irreversible de sus datos biométricos de cualquier base de datos, salvo obligación legal de conservación.

c) No ser sometida a identificación biométrica remota en espacios de acceso

público sin su conocimiento, salvo las excepciones estrictamente previstas en esta ley.

d) No ser objeto de categorización biométrica basada en características protegidas.

e) Obtener una explicación comprensible cuando una decisión que le afecte se base total o parcialmente en datos biométricos.

f) Impugnar toda identificación biométrica errónea y obtener la rectificación o eliminación de los registros inexactos.

Estos derechos son irrenunciables y toda cláusula contractual que implique su renuncia será nula de nulidad absoluta.

TÍTULO III — CONSENTIMIENTO Y BASES LEGALES

ARTÍCULO 6º — *Consentimiento biométrico reforzado.*

El consentimiento para la recolección y tratamiento de datos biométricos deberá ser:

a) Libre, previo, informado, específico, expreso y documentado por escrito o medio electrónico equivalente.

b) Otorgado para cada finalidad específica; el consentimiento genérico no será válido.

c) Precedido de información clara y accesible sobre: los tipos de datos biométricos a recolectar; la tecnología utilizada; las finalidades específicas; el período de conservación; los riesgos de seguridad; los derechos del titular; y la existencia de procesamiento automatizado o elaboración de perfiles.

d) Revocable en cualquier momento, debiendo el responsable proceder a la eliminación de los datos dentro de los diez (10) días hábiles.

No será válido el consentimiento cuando se condicione la prestación de un servicio, el acceso a un establecimiento, la celebración de un contrato o el acceso o permanencia en un empleo a la entrega de datos biométricos, salvo que el tratamiento biométrico sea estrictamente necesario para la prestación del servicio específico.

ARTÍCULO 7º — *Excepciones al consentimiento.*

Podrán tratarse datos biométricos sin consentimiento exclusivamente en los siguientes

supuestos taxativos:

a) Cumplimiento de obligaciones legales específicas que exijan la identificación biométrica, tales como la expedición de documentos de identidad, pasaportes o registro de personas.

b) Verificación biométrica en contextos de seguridad crítica, limitados taxativamente a: zonas de embarque y desembarque de aeropuertos y aeródromos internacionales; centrales nucleares y radiactivas; instalaciones militares de las Fuerzas Armadas; sedes de almacenamiento de material clasificado conforme la legislación de defensa; y centros de datos del sector público que alojen información de seguridad nacional. La reglamentación no podrá ampliar esta enumeración. Todo uso de verificación biométrica en estos contextos deberá respetar el principio de proporcionalidad, aplicar medidas de minimización de datos y ofrecer, cuando sea operativamente viable, una alternativa no biométrica de verificación. La tercerización de la operación de sistemas biométricos en contextos de seguridad crítica no eximirá al organismo público contratante de las obligaciones y responsabilidades establecidas en la presente ley; el organismo será solidariamente responsable con el operador privado por el cumplimiento de todas las disposiciones aplicables.

c) Emergencia médica en que la persona se encuentre imposibilitada de consentir, limitado a la identificación del paciente.

d) Investigación penal mediante orden judicial fundada conforme el artículo 14 de la presente ley.

e) Búsqueda de personas desaparecidas o extraviadas, mediante resolución judicial o de la autoridad competente, limitada al fin específico y con eliminación de los datos una vez cumplido el objetivo.

TÍTULO IV — PROHIBICIONES

ARTÍCULO 8º — *Prácticas prohibidas.*

Quedan absolutamente prohibidas las siguientes prácticas:

a) La vigilancia biométrica masiva en espacios de acceso público, conforme la definición del artículo 3 inciso k) de la presente ley.

b) La construcción o expansión de bases de datos biométricos mediante la extracción automatizada no dirigida (scraping) de imágenes faciales u otros datos biométricos de internet, redes sociales, sistemas de videovigilancia o cualquier otra fuente, sin consentimiento específico de cada persona. Se entiende por extracción automatizada no dirigida la recolección sistemática de datos biométricos mediante herramientas automatizadas que operan sin individualización previa de los titulares cuyos datos se pretende obtener.

c) La categorización biométrica de personas según raza, origen étnico, orientación sexual, identidad de género, convicciones religiosas, opiniones políticas o afiliación sindical.

d) El reconocimiento de emociones en entornos laborales y educativos, salvo fines médicos o de seguridad estrictamente necesarios con consentimiento explícito.

e) La comercialización, venta, cesión onerosa o intercambio de bases de datos biométricos con fines publicitarios, de perfilamiento comercial o de marketing.

f) El condicionamiento del acceso a servicios públicos esenciales (salud, educación, transporte, prestaciones sociales) a la identificación biométrica cuando exista un medio alternativo de identificación.

g) La recolección encubierta de datos biométricos, es decir, sin que la persona sea informada de manera clara, visible y previa.

h) El uso de datos biométricos de menores de dieciséis (16) años con fines distintos a los estrictamente terapéuticos, de identificación para documentos oficiales, o de seguridad en establecimiento educativo con consentimiento parental verificado.

Las prohibiciones del presente artículo son de orden público y no admiten excepción por vía reglamentaria.

ARTÍCULO 9º — *Acción de protección biométrica.*

Toda persona que considere que sus datos biométricos son o serán recolectados, almacenados, procesados o utilizados en violación de la presente ley podrá interponer una acción de protección biométrica de trámite sumarísimo ante el juez competente. La acción procederá tanto de manera preventiva como reparatoria. El juez deberá resolver la medida cautelar dentro de las veinticuatro (24) horas de presentada la solicitud

cuando exista riesgo de daño inminente o irreparable.

Tendrán legitimación activa:

a) El titular de los datos biométricos.

b) El Defensor del Pueblo de la Nación o sus equivalentes provinciales.

c) Las asociaciones de defensa de consumidores registradas.

d) Las organizaciones de la sociedad civil cuyo objeto estatutario incluya la protección de derechos digitales, la privacidad o los derechos humanos.

e) La Autoridad Nacional de Protección de Datos Personales (ANPDP).

Será procedente la acción colectiva cuando la violación afecte a una pluralidad de personas, incluyendo cuando el sistema biométrico opera en espacios de acceso público. En las acciones de protección biométrica relativas a sistemas de identificación biométrica remota operados sin consentimiento o sin autorización judicial, se invertirá la carga de la prueba: corresponderá al operador demostrar la licitud del tratamiento, la existencia de base legal y el cumplimiento de las obligaciones de la presente ley.

ARTÍCULO 10º — *Delitos biométricos.*

Incorpóranse como artículos 157 ter, 157 quáter, 157 quinquies y 157 sexies del Código Penal de la Nación (Título V, Capítulo III, "Violación de secretos y de la privacidad") los siguientes:

"Artículo 157 ter: Será reprimido con prisión de seis (6) meses a tres (3) años el que, mediante herramientas automatizadas y sin consentimiento de los titulares, recolectare datos biométricos de manera sistemática y no dirigida de internet, redes sociales, sistemas de videovigilancia u otras fuentes accesibles por medios informáticos, con el fin de construir, ampliar o alimentar bases de datos biométricos."

"Artículo 157 quáter: Será reprimido con prisión de uno (1) a cinco (5) años el que comercializare, vendiere, cediere onerosamente o intercambiare bases de datos que contengan datos biométricos de terceros. La pena se elevará en un tercio cuando la base contenga datos de menores de dieciocho (18) años."

"Artículo 157 quinquies: Será reprimido con prisión de dos (2) a seis (6) años el funcionario público que desplegare, autorizare o consintiere el despliegue de sistemas de vigilancia biométrica masiva en espacios de acceso público conforme la definición del artículo 3 inciso k) de la Ley de Protección de Datos Biométricos y Regulación del

Reconocimiento Facial, o que utilizare sistemas de identificación biométrica remota sin la autorización judicial previa exigida por dicha ley."

"Artículo 157 sexies: Será reprimido con prisión de uno (1) a cuatro (4) años el que, sin autorización del titular de los datos o del responsable del tratamiento, accediere, copiare, alterare, destruyere o divulgare datos biométricos almacenados en bases de datos. Cuando el delito fuere cometido por un funcionario público en ejercicio o con ocasión de sus funciones, la pena se incrementará en un medio."

ARTÍCULO 11º — *Soberanía biométrica.*

Las bases de datos biométricos del sector público nacional, provincial y municipal deberán almacenarse primariamente en servidores ubicados en territorio argentino. La transferencia internacional de datos biométricos solo procederá conforme el régimen de la Ley de Protección Integral de Datos Personales y requerirá, adicionalmente, autorización expresa de la ANPDP cuando se trate de bases de más de cien mil (100.000) registros biométricos.

Se prohíbe la transferencia internacional de datos biométricos recolectados por fuerzas de seguridad, salvo en el marco de convenios de cooperación judicial internacional ratificados por ley del Congreso.

La contratación de proveedores extranjeros de tecnología biométrica por el sector público deberá incluir cláusulas de auditoría, control de acceso y prohibición de extracción o copia de datos biométricos fuera del territorio nacional, bajo responsabilidad solidaria del organismo contratante.

TÍTULO V — USO POR FUERZAS DE SEGURIDAD Y SECTOR PÚBLICO

ARTÍCULO 12º — *Principio de excepcionalidad.*

El uso de sistemas de identificación biométrica por fuerzas de seguridad y organismos del sector público es excepcional, de interpretación restrictiva y solo procederá conforme las disposiciones del presente Título. Ningún sistema de identificación biométrica remota podrá ser desplegado por fuerzas de seguridad sin autorización judicial previa.

ARTÍCULO 13º — *Uso dirigido de identificación biométrica por fuerzas de seguridad.*

Nada en la presente ley impide a las fuerzas de seguridad el uso de sistemas de identificación biométrica de carácter dirigido, entendido como la comparación de datos biométricos de una persona determinada con bases de datos en el marco de una investigación penal con orden judicial. Este uso no constituye vigilancia biométrica masiva en los términos del artículo 3 inciso k).

ARTÍCULO 14º — *Autorización judicial para identificación biométrica remota.*

La identificación biométrica remota en tiempo real en espacios de acceso público por fuerzas de seguridad solo podrá autorizarse mediante resolución judicial fundada, individualmente motivada, cuando concurran acumulativamente los siguientes requisitos:

a) Investigación de delitos graves con pena mínima de diez (10) años de prisión, o búsqueda dirigida de víctimas de secuestro, trata de personas o personas desaparecidas.

b) Existencia de indicios graves, concretos y actuales que justifiquen la medida.

c) Agotamiento o inviabilidad demostrada de medios de investigación menos invasivos.

d) Delimitación precisa del ámbito espacial y temporal de la medida, que no podrá exceder de setenta y dos (72) horas, renovable por igual período previa nueva autorización judicial.

e) Designación de un responsable de la operación que garantice la supervisión humana continua y la eliminación inmediata de los datos de personas no buscadas.

La autorización judicial deberá especificar la persona o personas buscadas, el delito investigado, la zona geográfica, la duración, la tecnología a utilizar y las medidas de protección de datos de terceros.

La identificación biométrica remota posterior (no en tiempo real) por fuerzas de seguridad requerirá igualmente autorización judicial, con las garantías previstas en este artículo.

ARTÍCULO 15º — *Registro de operaciones biométricas de seguridad.*

Todo uso de identificación biométrica por fuerzas de seguridad deberá registrarse ante la Autoridad de Aplicación, incluyendo: la autorización judicial; la tecnología utilizada; la

duración y alcance; el número de personas escaneadas; los resultados positivos y falsos positivos detectados; y las medidas de eliminación de datos adoptadas. La Autoridad de Aplicación publicará un informe estadístico semestral, anonimizado, sobre el uso de estas tecnologías por fuerzas de seguridad.

ARTÍCULO 16º — *Evaluación de impacto en derechos fundamentales.*

Todo organismo del sector público que pretenda implementar un sistema de identificación o verificación biométrica de riesgo medio o alto conforme el artículo 3 inciso m) deberá realizar, con carácter previo, una evaluación de impacto en derechos fundamentales que incluya: análisis de necesidad y proporcionalidad; identificación de riesgos de discriminación y sesgos algorítmicos; medidas de mitigación; período de prueba supervisado; y mecanismo de reclamo accesible. La evaluación deberá presentarse ante la Autoridad de Aplicación con al menos sesenta (60) días de anticipación a la implementación.

La evaluación seguirá la metodología y estándares técnicos que establezca la ANPDP mediante resolución fundada, los cuales incluirán como mínimo:

a) Métricas de precisión obligatorias: tasa de falsos positivos, tasa de falsos negativos, tasa de error diferencial por género, edad y tono de piel, conforme estándares internacionales (ISO/IEC 19795 o equivalente).

b) Umbrales máximos de error admisibles para cada contexto de uso, que serán más estrictos para usos con efectos jurídicos sobre las personas.

c) Protocolo de prueba con conjuntos de datos demográficamente representativos de la población argentina.

d) Análisis de alternativas menos invasivas con evaluación comparativa de efectividad.

La ANPDP publicará y actualizará bienalmente las guías metodológicas de evaluación de impacto biométrico, que serán de cumplimiento obligatorio.

ARTÍCULO 17º — *Prohibición de uso como prueba única.*

Ninguna persona podrá ser detenida, procesada o condenada sobre la base exclusiva de una identificación biométrica automatizada. La identificación biométrica podrá ser utilizada como elemento indiciario, pero deberá ser corroborada por otros medios de prueba independientes. Toda identificación biométrica utilizada en un proceso penal

deberá ir acompañada de un informe sobre la tasa de error del sistema, la calidad de la muestra y las condiciones de captura.

TÍTULO VI — USO EN EL SECTOR PRIVADO

ARTÍCULO 18º — *Régimen general y proporcionalidad.*

El uso de datos biométricos por el sector privado se regirá por el consentimiento biométrico reforzado del artículo 6 y las prohibiciones del artículo 8. Las obligaciones regulatorias se aplicarán de manera proporcionada al nivel de riesgo biométrico conforme el artículo 3 inciso m):

a) Riesgo bajo: los operadores de sistemas de verificación biométrica uno a uno con procesamiento local y consentimiento cumplirán las obligaciones generales de la presente ley, sin requerir registro ni evaluación de impacto.

b) Riesgo medio: los operadores de sistemas de identificación biométrica con bases de datos de hasta diez mil (10.000) registros cumplirán, adicionalmente, la obligación de registro del artículo 19 y realizarán una evaluación de impacto simplificada conforme las guías de la ANPDP.

c) Riesgo alto: los operadores de sistemas de identificación biométrica con bases superiores a diez mil (10.000) registros, sistemas remotos o sistemas con efectos jurídicos directos cumplirán, adicionalmente, la obligación de auditoría de sesgos del artículo 20 y la evaluación de impacto completa.

Adicionalmente, en todos los niveles de riesgo:

d) Todo sistema de verificación biométrica utilizado en relaciones de consumo deberá ofrecer una alternativa no biométrica de identificación, sin pérdida de funcionalidades esenciales ni trato diferenciado perjudicial.

e) Los datos biométricos recolectados con fines de verificación de identidad (desbloqueo de dispositivos, acceso a cuentas, autenticación de pagos) deberán procesarse localmente (on-device) cuando la tecnología lo permita, minimizando la transferencia a servidores externos.

f) Queda prohibido condicionar la relación laboral a la provisión de datos biométricos más allá de los estrictamente necesarios para el control de acceso al lugar de trabajo, conforme la legislación laboral vigente.

ARTÍCULO 19º — *Registro de sistemas biométricos privados.*

Todo operador del sector privado que implemente un sistema de identificación biométrica de riesgo medio o alto (comparación uno a muchos) deberá inscribirlo en el Registro Nacional de Sistemas Biométricos que administrará la Autoridad de Aplicación, informando: descripción del sistema y tecnología; finalidad específica; base legal; categorías de datos; período de conservación; medidas de seguridad; y evaluación de impacto cuando sea exigible. El registro se tramitará mediante declaración jurada en formato digital, con silencio administrativo positivo a los treinta (30) días hábiles de presentada la declaración completa.

Los sistemas de verificación biométrica (comparación uno a uno) de uso común quedarán exceptuados del registro, sin perjuicio de las demás obligaciones de la presente ley.

ARTÍCULO 20º — *Auditoría de sesgos.*

Los operadores de sistemas de identificación biométrica de riesgo alto que afecten a más de diez mil (10.000) personas anuales deberán realizar auditorías anuales de sesgos que evalúen las tasas de error diferenciadas por género, edad, tono de piel y otras variables relevantes. Los resultados serán comunicados a la Autoridad de Aplicación y publicados en formato accesible. Las micro, pequeñas y medianas empresas (MiPyMEs) podrán acreditar el cumplimiento de esta obligación mediante auditorías realizadas por el proveedor del sistema biométrico, siempre que el auditor sea independiente del desarrollador.

Cuando la auditoría revele tasas de error desproporcionadamente elevadas para algún grupo, el operador deberá adoptar medidas correctivas dentro de los sesenta (60) días o suspender el uso del sistema respecto de dicho grupo hasta corregir el sesgo.

TÍTULO VII — SEGURIDAD Y ELIMINACIÓN

ARTÍCULO 21º — *Seguridad reforzada.*

Los datos biométricos requieren medidas de seguridad reforzadas, que incluirán como mínimo:

a) Cifrado de extremo a extremo en almacenamiento y transmisión.

b) Almacenamiento mediante plantillas biométricas (templates) irreversibles cuando sea técnicamente viable, en lugar de imágenes o datos biométricos brutos.

c) Segmentación de las bases de datos biométricos respecto de otros datos personales.

d) Registros de acceso (logs) con identificación del operador, fecha, hora y finalidad de cada consulta.

e) Evaluaciones periódicas de vulnerabilidad y pruebas de penetración.

f) Plan de respuesta ante incidentes específico para datos biométricos.

ARTÍCULO 22º — *Eliminación.*

Los datos biométricos deberán eliminarse de manera segura e irreversible:

a) Cuando se haya cumplido la finalidad específica para la cual fueron recolectados.

b) Cuando el titular revoque su consentimiento, dentro de los diez (10) días hábiles.

c) Cuando la relación contractual o laboral que motivó la recolección haya finalizado, dentro de los treinta (30) días hábiles, salvo obligación legal de conservación.

d) Cuando lo ordene la Autoridad de Aplicación o un juez competente.

La eliminación comprenderá todas las copias, incluyendo respaldos, y se documentará mediante acta que el responsable conservará por cinco (5) años.

TÍTULO VIII — AUTORIDAD DE APLICACIÓN Y RÉGIMEN SANCIONATORIO

ARTÍCULO 23º — *Autoridad de Aplicación.*

Será Autoridad de Aplicación la Autoridad Nacional de Protección de Datos Personales (ANPDP), la cual ejercerá las funciones previstas en la presente ley con autonomía funcional, independencia de criterio técnico y autonomía financiera en la administración de los recursos que le asigne el presupuesto nacional y los que genere por vía de las tasas y multas previstas en esta ley.

La ANPDP creará un Área de Biometría y Vigilancia dentro de la Unidad Técnica de Inteligencia Artificial y Responsabilidad Algorítmica (UTIARA), dotada de especialistas en visión computacional, biometría, estadística aplicada y derechos humanos.

El Área de Biometría contará con presupuesto operativo diferenciado dentro de la ANPDP y una dotación mínima de diez (10) profesionales especializados. La ANPDP podrá celebrar convenios con universidades nacionales y el CONICET para la asistencia técnica permanente en evaluación de sistemas biométricos, auditoría de sesgos y desarrollo de estándares. Cuando la complejidad técnica lo requiera, la ANPDP podrá designar comisiones de expertos ad hoc para la evaluación de sistemas biométricos específicos.

Las decisiones técnicas de la ANPDP en materia biométrica no estarán sujetas a avocación ni a instrucción del Poder Ejecutivo Nacional. El titular de la ANPDP solo podrá ser removido por las causales y el procedimiento establecidos en la ley de creación de dicho organismo.

ARTÍCULO 24º — *Funciones específicas.*

La Autoridad de Aplicación tendrá, además de las funciones generales, las siguientes funciones específicas:

a) Administrar el Registro Nacional de Sistemas Biométricos.

b) Evaluar las evaluaciones de impacto en derechos fundamentales del sector público.

c) Supervisar el cumplimiento de la obligación de auditoría de sesgos.

d) Publicar el informe estadístico semestral sobre uso policial de biometría.

e) Emitir estándares técnicos de precisión mínima y tasas de error máximas admisibles para sistemas biométricos utilizados en decisiones con efectos jurídicos.

f) Certificar los sistemas biométricos que cumplan con los estándares de la presente ley.

g) Coordinar con el Poder Judicial para el cumplimiento del régimen de autorizaciones del Título V.

h) Administrar el Espacio Controlado de Pruebas Biométricas previsto en el Título X de la presente ley.

ARTÍCULO 25º — *Infracciones y sanciones.*

Se clasifican las infracciones en:

a) Leves: incumplimiento de obligaciones formales de registro, señalización o documentación. Sanción: apercibimiento y/o multa de hasta el cero coma cinco por ciento (0,5%) de la facturación bruta anual global o hasta quinientos (500) salarios mínimos, vitales y móviles (SMVM).

b) Graves: tratamiento sin consentimiento válido; omisión de evaluación de impacto; incumplimiento de obligaciones de seguridad o eliminación; uso de identificación biométrica sin registro; omisión de alternativa no biométrica. Sanción: multa de hasta el dos por ciento (2%) de la facturación bruta anual global o hasta cinco mil (5.000) SMVM.

c) Muy graves: vigilancia biométrica masiva; scraping de datos biométricos; categorización por características protegidas; uso policial sin autorización judicial; comercialización de bases biométricas; tratamiento ilícito de datos biométricos de menores. Sanción: multa de hasta el cuatro por ciento (4%) de la facturación bruta anual global o hasta veinte mil (20.000) SMVM; clausura del sistema; eliminación forzosa de la base de datos.

Adicionalmente, toda persona afectada por una violación de la presente ley tendrá derecho a indemnización conforme la legislación de responsabilidad civil aplicable y la Ley de Protección Integral de Datos Personales. Los datos biométricos se considerarán datos sensibles a todos los efectos indemnizatorios.

TÍTULO IX — DESARROLLO ESTRATÉGICO BIOMÉTRICO NACIONAL

ARTÍCULO 26º — *Política nacional de desarrollo biométrico responsable.*

Decárase de interés nacional el desarrollo de una industria biométrica argentina responsable, soberana y competitiva. El Estado Nacional promoverá la investigación, el desarrollo y la producción nacional de tecnologías biométricas que cumplan con los estándares de la presente ley, con el objetivo de reducir la dependencia de proveedores extranjeros, generar empleo de alta calificación y posicionar a la Argentina como referente regional en biometría ética.

ARTÍCULO 27º — *Espacio Controlado de Pruebas Biométricas (sandbox regulatorio).*

Créase el Espacio Controlado de Pruebas Biométricas (ECPB), administrado por la ANPDP, destinado a permitir el desarrollo y testeo de tecnologías biométricas innovadoras en un entorno regulatorio supervisado.

El ECPB se regirá por las siguientes reglas:

a) Podrán participar empresas, universidades, centros de investigación y organismos públicos que presenten proyectos de innovación biométrica responsable.

b) La participación será voluntaria, gratuita para MiPyMEs y organismos públicos, y por un plazo máximo de doce (12) meses, prorrogable por única vez.

c) Los participantes podrán solicitar la flexibilización temporaria de las obligaciones de registro y evaluación de impacto, manteniendo íntegramente las prohibiciones del artículo 8, las obligaciones de consentimiento del artículo 6 y los requisitos de seguridad del artículo 21.

d) Todo dato biométrico recolectado en el ECPB deberá eliminarse al finalizar el período de prueba, salvo consentimiento explícito del titular para su conservación en condiciones operativas.

e) La ANPDP publicará un informe anual con los resultados agregados del ECPB y las recomendaciones regulatorias derivadas de la experiencia acumulada.

ARTÍCULO 28º — *Integración con el ecosistema científico-tecnológico.*

El Ministerio de Ciencia, Tecnología e Innovación, en coordinación con la ANPDP, promoverá:

a) La articulación de INVAP S.E., ARSAT S.A., el CONICET y las universidades nacionales para el desarrollo de soluciones biométricas soberanas, priorizando el procesamiento local, la reducción de sesgos y la protección de la privacidad por diseño.

b) La creación de líneas de financiamiento específicas para MiPyMEs de base tecnológica que desarrollen soluciones biométricas conformes a los estándares de la presente ley, a través de la Agencia Nacional de Promoción de la Investigación, el Desarrollo Tecnológico y la Innovación (Agencia I+D+i) y del Fondo Fiduciario de Promoción de la Industria del Software (FONSOFT) o el instrumento que lo reemplace.

c) La incorporación de la biometría ética como línea prioritaria en las

convocatorias del Fondo para la Investigación Científica y Tecnológica (FONCyT).

d) La preferencia, en las contrataciones públicas de tecnología biométrica, de soluciones de desarrollo nacional que cumplan con los estándares de la presente ley y permitan la auditoría integral del código fuente y los algoritmos.

ARTÍCULO 29º — *Interoperabilidad y estándares nacionales.*

La ANPDP, en consulta con el Instituto Argentino de Normalización y Certificación (IRAM) y los organismos técnicos competentes, establecerá estándares nacionales de interoperabilidad biométrica que garanticen:

a) La compatibilidad técnica entre los sistemas biométricos del sector público nacional, provincial y municipal, evitando la fragmentación y la duplicación de bases de datos.

b) La portabilidad de las plantillas biométricas entre sistemas certificados, permitiendo al titular migrar sus datos sin necesidad de nueva captura.

c) La adopción de protocolos de identidad digital segura basados en estándares abiertos, que integren la verificación biométrica como capa opcional y voluntaria.

d) La alineación con los estándares internacionales ISO/IEC 19794 (formatos de datos biométricos) e ISO/IEC 30107 (detección de ataques de presentación).

TÍTULO X — DISPOSICIONES COMPLEMENTARIAS Y TRANSITORIAS

ARTÍCULO 30º — *Coordinación normativa.*

La presente ley se aplicará complementaria y coordinadamente con la Ley de Protección Integral de Datos Personales, y con la legislación vigente o en trámite parlamentario en materia de neuroderechos, responsabilidad civil por daños de sistemas de inteligencia artificial, soberanía cognitiva y toda otra normativa aplicable. En caso de conflicto, prevalecerá la norma que otorgue mayor protección a los derechos de las personas.

ARTÍCULO 31º — *Cláusula pro-innovación.*

La presente ley no tiene por objeto prohibir la innovación biométrica responsable. La verificación biométrica con consentimiento, el procesamiento local, la investigación científica con datos anonimizados, el desarrollo de tecnologías de mejora de precisión y

reducción de sesgos, y la participación en el Espacio Controlado de Pruebas Biométricas quedan explícitamente permitidos y promovidos.

ARTÍCULO 32º — *Informe de impacto regulatorio PyME.*

Dentro de los ciento ochenta (180) días de la entrada en vigencia de la presente ley, la ANPDP publicará un informe de impacto regulatorio que evalúe la carga que las obligaciones de la presente ley imponen a las MiPyMEs y propondrá, en su caso, medidas de simplificación administrativa. Dicho informe se actualizará bienalmente.

ARTÍCULO 33º — *Cláusula de revisión tecnológica (sunset clause).*

El Congreso de la Nación realizará una revisión integral de la presente ley dentro de los cinco (5) años de su entrada en vigencia, a fin de evaluar la adecuación de sus disposiciones a la evolución tecnológica, la experiencia regulatoria acumulada y los estándares internacionales vigentes. La Autoridad de Aplicación elevará al Congreso un informe técnico con recomendaciones al menos seis (6) meses antes del vencimiento del plazo.

ARTÍCULO 34º — *Revisión de sistemas existentes.*

Los organismos públicos y privados que al momento de la entrada en vigencia de la presente ley operen sistemas de identificación biométrica dispondrán de doce (12) meses para adecuarse a sus disposiciones, inscribirse en el Registro y realizar la evaluación de impacto cuando corresponda. Los sistemas de vigilancia biométrica masiva prohibidos por el artículo 8 deberán desactivarse dentro de los sesenta (60) días de la entrada en vigencia.

ARTÍCULO 35º — *Reglamentación.*

El Poder Ejecutivo Nacional reglamentará la presente ley dentro de los ciento ochenta (180) días de su publicación.

ARTÍCULO 36º — *Vigencia.*

La presente ley entrará en vigencia a los noventa (90) días de su publicación en el Boletín Oficial.

ARTÍCULO 37º — *Comunicación.*

Comuníquese al Poder Ejecutivo.

LIC. MARCELA MARINA PAGANO

DIPUTADA DE LA NACIÓN

DIPUTADOS
ARGENTINA

FUNDAMENTOS

Señor Presidente:

I. El problema. Los datos biométricos son, por su naturaleza, irrevocables. A diferencia de una contraseña o un documento de identidad, un rostro, una huella dactilar o un patrón de iris no pueden ser reemplazados si son comprometidos. Esta característica única exige un nivel de protección proporcionalmente excepcional. Sin embargo, la Argentina carece de legislación específica sobre datos biométricos. La Ley 25.326 no los menciona. Los sistemas de reconocimiento facial se despliegan en el país por fuerzas de seguridad nacionales y provinciales, en aeropuertos, estadios y espacios públicos, sin marco legal específico, sin autorización judicial sistemática, sin evaluaciones de impacto y sin mecanismos de control independiente.

II. El contexto global. El mundo se ha dividido en tres campos. La Unión Europea prohibió la identificación biométrica remota en tiempo real en espacios públicos desde febrero de 2025 mediante el AI Act, con excepciones estrechas y autorización judicial. En Estados Unidos, Illinois obtuvo mediante su BIPA acuerdos judiciales de miles de millones de dólares contra Facebook, Google y Meta por recolección de datos biométricos sin consentimiento; quince estados tienen restricciones diversas; y dieciséis ciudades han prohibido el uso policial de reconocimiento facial. La mayoría de América Latina, incluida Argentina, opera sin reglas.

III. La arquitectura del proyecto. El proyecto de treinta y siete (37) artículos en diez (10) Títulos establece un régimen integral que opera en tres niveles: prohibiciones absolutas para las prácticas más invasivas (vigilancia masiva, scraping, categorización discriminatoria, reconocimiento de emociones laboral/educativo); un régimen de autorización judicial estricta para el uso policial de biometría remota; y un régimen de consentimiento reforzado con enfoque basado en riesgo para el sector privado.

Cinco innovaciones distinguen este proyecto. Primera, la distinción explícita entre identificación (uno a muchos, alto riesgo) y verificación (uno a uno, menor riesgo), con regímenes regulatorios diferenciados que evitan sobrerregular el desbloqueo de dispositivos o la autenticación de pagos. Segunda, la auditoría de sesgos obligatoria con publicación de resultados, que atiende el problema documentado de tasas de error desproporcionadas para mujeres y personas de tez oscura. Tercera, la prohibición de

uso como prueba única en procesos penales, que reconoce la falibilidad inherente de estos sistemas. Cuarta, la cláusula pro-innovación explícita que protege la verificación con consentimiento, el procesamiento local y la investigación científica. Quinta, el enfoque basado en riesgo que escala las obligaciones regulatorias proporcionalmente al impacto del sistema, protegiendo a las MiPyMEs de cargas excesivas sin debilitar la protección de derechos.

IV. Integración sistémica. El proyecto se inserta en el Sistema Argentino de Gobernanza de Inteligencia Artificial como pieza del ecosistema legislativo impulsado por esta representación, coordinado con la Ley de Protección Integral de Datos Personales (que define los datos biométricos como sensibles) y con los proyectos de ley presentados por esta Diputación en materia de neuroderechos (que cubren los neurodatos biométricos), responsabilidad civil por daños de sistemas de inteligencia artificial (que establece responsabilidad objetiva para sistemas biométricos de alto riesgo) y soberanía cognitiva (que protege la autonomía frente a algoritmos de perfilamiento). La Autoridad de Aplicación es la misma ANPDP con su UTIARA, garantizando coherencia institucional.

V. Viabilidad política. El proyecto adopta un enfoque equilibrado: prohíbe lo que debe prohibirse (vigilancia masiva, scraping, discriminación), regula estrictamente lo que requiere control judicial (uso policial), y permite lo que beneficia a las personas (verificación con consentimiento, innovación responsable). Las auditorías de sesgos y la publicación de estadísticas de uso policial generan transparencia sin impedir el uso legítimo de la tecnología. El enfoque basado en riesgo evita que la regulación se convierta en barrera de entrada para PyMEs y startups tecnológicas, al reservar las cargas más exigentes para los sistemas de mayor impacto.

VI. Incorporación al Código Penal. El artículo 10 del presente proyecto incorpora cuatro tipos penales como artículos 157 ter, 157 quáter, 157 quinquies y 157 sexies del Código Penal de la Nación, dentro del Título V (“Delitos contra la libertad”), Capítulo III (“Violación de secretos y de la privacidad”). Esta ubicación sistémica es coherente con los artículos 153 a 157 bis vigentes, que protegen la privacidad de las comunicaciones y los datos personales. Los nuevos tipos extienden esa protección a los datos biométricos, reconociendo que su vulneración constituye una afrenta particularmente grave a la intimidad personal dada la irrevocabilidad del dato comprometido. Cada tipo penal ha sido redactado con elementos típicos precisos y verificables: el scraping requiere automatización, sistematicidad y finalidad de alimentar bases de datos; la vigilancia

masiva se define por remisión a los criterios operativos del artículo 3 inciso k); y el acceso ilegítimo exige la ausencia de autorización del titular o del responsable.

VII. La dimensión económica: soberanía biométrica como política industrial. Este proyecto no es solo una ley de derechos: es una ley de desarrollo. La biometría es infraestructura económica crítica. Los flujos de identidad digital son tan estratégicos como los flujos de energía o de datos. Quien controla la identificación biométrica controla el acceso a servicios financieros, salud, transporte y gobierno digital. Hoy, la Argentina importa prácticamente toda su tecnología biométrica. Cada sistema de reconocimiento facial desplegado por el Estado con tecnología extranjera envía datos soberanos a servidores controlados por empresas sin jurisdicción argentina.

El Título IX del proyecto establece tres instrumentos para revertir esta dependencia. Primero, un sandbox regulatorio (Espacio Controlado de Pruebas Biométricas) que permite a empresas argentinas innovar con menores cargas burocráticas, manteniendo intactas las garantías de derechos. Segundo, la integración con INVAP, ARSAT, CONICET y el sistema universitario para desarrollar tecnología biométrica nacional con financiamiento específico a través de Agencia I+D+i y FONSOFT. Tercero, estándares nacionales de interoperabilidad que impidan la fragmentación y generen un mercado interno integrado.

La experiencia internacional demuestra que los países que regulan primero la biometría capturan la ventaja competitiva: las empresas que cumplen estándares estrictos acceden a mercados globales que exigen esos mismos estándares. La regulación no es un costo: es una ventaja competitiva. Argentina tiene la oportunidad de posicionarse como líder regional en biometría ética, exportando soluciones certificadas a una América Latina que hoy carece de marcos regulatorios propios.

Por todo lo expuesto, solicito a mis pares la aprobación del presente proyecto de ley.

LIC. MARCELA MARINA PAGANO

DIPUTADA DE LA NACIÓN