CENTRAN

CENTRO DE TRANSFORMACIÓN NACIONAL PARA LA VERDAD, LA JUSTICIA Y LA LIBERTAD

CENTRANVE.ORG | REPÚBLICA BOLIVARIANA DE VENEZUELA | ASAMBLEA NACIONAL

Ref.: CENTRAN-PLEY-LOPDP-2026-002

Elaborado por: Unidad de Investigación y Documentación CENTRAN

PROYECTO DE LEY ORGÁNICA
DE PROTECCIÓN DE DATOS PERSONALES

VERSIÓN 1.5 (CONSOLIDADA)

BORRADOR CONSOLIDADO PARA CONSULTA TÉCNICA, JURÍDICA E INSTITUCIONAL

DESTINO INSTITUCIONAL

Preparado para consulta técnica, jurídica e institucional y para una eventual presentación ante la Asamblea Nacional, una vez culminado el proceso de reinstitucionalización democrática y constituido un nuevo gobierno elegido democráticamente en Venezuela.

ADVERTENCIA SOBRE DESTINATARIOS

La mención de personas, mesas, partidos, universidades, colegios y organizaciones destinatarias tiene finalidad exclusivamente consultiva; no implica adhesión, aval, participación en la redacción ni atribución de posición institucional.

Caracas | Granada (España) | Miami (EE. UU.) | Noviembre de 2026

PRESENTACIÓN INSTITUCIONAL

Ref.: CENTRAN-PLEY-LOPDP-2026-002 | Versión: 1.5 (Consolidada — revisión consultiva)

Elaborado por: Unidad de Investigación y Documentación CENTRAN | Caracas, Granada (España), Miami (EE. UU.), noviembre de 2026.

Destinado: consulta técnica, jurídica e institucional y eventual presentación ante la Asamblea Nacional que se constituya tras la culminación del proceso de reinstitucionalización democrática y la elección de un nuevo gobierno democrático en Venezuela.

CONTENIDO NORMATIVO	EJES DE CONSULTA
La V1.5 se organiza en catorce títulos y ciento cuarenta y tres artículos, incluidos los artículos 2 bis, 4 bis, 25 bis y 44 bis; diez disposiciones transitorias; una disposición derogatoria y cuatro disposiciones finales.	Protección de categorías especiales y biometría; derechos de las personas; autoridad de control; habeas data; gobernanza algorítmica e IA; derechos digitales; videovigilancia; transferencias internacionales y régimen sancionador.

DESTINATARIOS Y ESPACIOS DE DELIBERACIÓN

La consulta se propone, por una parte, a la mesa de trabajo presidida por Dinorah Figuera, vinculada a la Asamblea Nacional electa en 2015; y, por separado, a la Presidencia y a los equipos técnicos y jurídicos de la Asamblea Nacional instalada en enero de 2026 tras las elecciones parlamentarias de 2025, presidida por Jorge Rodríguez para el período anual 2026-2027, conforme al Acuerdo publicado en la Gaceta Oficial N.º 43.288, de 5 de enero de 2026. También se propone consultar a colegios de abogados, facultades de Derecho, universidades, colegios profesionales, equipos técnicos y jurídicos de partidos políticos, representantes del entorno de María Corina Machado, especialistas en informática, protección de datos y ciberseguridad, organizaciones de derechos humanos y de la sociedad civil, sectores empresarial y tecnológico y demás personas interesadas. La identificación de estos destinatarios tiene finalidad exclusivamente consultiva y no implica adhesión, aval, participación en la redacción ni atribución de posición institucional.

> NATURALEZA JURÍDICA. La V1.5 es un borrador de trabajo para consulta y deliberación. No constituye una ley aprobada, un texto oficialmente consignado ni un cierre legislativo. Las referencias comparadas no atribuyen automáticamente competencias a autoridades venezolanas.

Criterio de lectura. La ficha anterior es introductoria. A continuación se reproduce el texto consolidado de la Versión 1.5, con integración de recomendaciones adicionales del Informe Técnico-Jurídico Comparativo y de Consolidación. Las propuestas institucionales y de técnica legislativa se someten a deliberación y no constituyen dictamen constitucional vinculante.

ESTRUCTURA DEL PROYECTO

Catorce títulos · 143 artículos, incluidos los artículos 2 bis, 4 bis, 25 bis y 44 bis · Disposiciones transitorias, derogatoria y finales

TÍTULO I	**DISPOSICIONES GENERALES**
TÍTULO II	**PRINCIPIOS RECTORES DEL TRATAMIENTO**
TÍTULO III	**BASES DE LEGITIMACIÓN DEL TRATAMIENTO**
TÍTULO IV	**CATEGORÍAS ESPECIALES DE DATOS**
TÍTULO V	**DERECHOS DEL INTERESADO**
TÍTULO VI	**OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO**
TÍTULO VII	**HABEAS DATA**
TÍTULO VIII	REGISTRO NACIONAL DE TRATAMIENTOS DE DATOS PERSONALES
TÍTULO IX	**GOBERNANZA ALGORÍTMICA E INTELIGENCIA ARTIFICIAL**
TÍTULO X	**DERECHOS DIGITALES LABORALES**
TÍTULO XI	**RÉGIMEN GENERAL DE VIDEOVIGILANCIA Y TECNOLOGÍAS DE CONTROL**
TÍTULO XII	**DERECHOS DIGITALES DEL CIUDADANO**
TÍTULO XIII	**TRANSFERENCIAS INTERNACIONALES DE DATOS**
TÍTULO XIV	**SUPERINTENDENCIA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES**

DOCUMENTOS DE CIERRE

Disposiciones transitorias (diez) • Disposición derogatoria (una) • Disposiciones finales (cuatro) • Anexo I: fuentes normativas y documentales para la consulta.

PARTE I

GUÍA DE CAMBIOS Y CONSOLIDACIÓN SOBRE LA V1.4

La presente Versión 1.5 consolida y fortalece el Proyecto de Ley Orgánica de Protección de Datos Personales a partir de la V1.4, incorporando el análisis del Informe de Adecuación de 4 de noviembre de 2026, la revisión constitucional y la armonización técnica del articulado. Se presenta como borrador para consulta técnica, jurídica e institucional; no constituye ley aprobada, texto oficialmente consignado ni cierre legislativo.

1. Reformas sustantivas integradas

1.1. Autoridad de control, independencia y rendición de cuentas

Se propone una Superintendencia como ente público de derecho, con personalidad jurídica y patrimonio propios, autonomía funcional, técnica, administrativa, financiera y de personal, configurada como autoridad administrativa independiente de supervisión. No se la presenta como un sexto Poder Público ni como entidad situada fuera del orden constitucional. Se incorpora un modelo de independencia funcional con vinculación administrativa instrumental —sin tutela sobre expedientes ni instrucciones de fondo—, control fiscal externo, rendición de cuentas parlamentaria y control jurisdiccional. La ubicación orgánica definitiva queda sujeta a dictamen constitucional y deliberación legislativa.

1.2. Legalidad sancionatoria y reserva de ley

Se sustituye la tipificación abierta por un catálogo legal cerrado; se prohíbe crear infracciones, categorías sancionables o sanciones mediante reglamento; se refuerzan presunción de inocencia, culpabilidad, defensa, proporcionalidad, non bis in idem, prescripción y separación entre instrucción y decisión; y se distingue el reglamento general de las normas técnicas de la autoridad de control.

1.3. Derechos constitucionales, tutela judicial y garantías de grupos protegidos

Se amplían los anclajes constitucionales, se incorporan salvaguardas para libertad de expresión, periodismo, archivos e investigación, se ajusta el régimen de niños, niñas y adolescentes al principio de autonomía progresiva y a la LOPNNA, se precisa el hábeas data y se incorporan reglas de reparación por daños.

1.4. Biometría estatal, seguridad, empleo y transiciones

Se preserva el régimen biométrico reforzado de la V1.4 y se añaden reglas para identificación civil, electoral y consular, servicios públicos, geolocalización laboral, dispositivos del empleador, notificación de brechas con riesgo vital y tratamiento de datos de víctimas y testigos. Se distinguen prácticas prohibidas desde la entrada en vigor de los sistemas preexistentes que puedan someterse a auditoría y adecuación, sin presunción de licitud.

1.5. Registro, transferencias, alcance territorial y técnica legislativa

Se hace tecnológicamente neutral el Registro Nacional de Tratamientos, se limita la publicidad a campos no sensibles, se incorpora el tratamiento estatal en el exterior y se precisan garantías para transferencias internacionales, derogación expresa y calendario de implantación.

2. Decisiones abiertas para la consulta institucional

La consulta deberá pronunciarse especialmente sobre: (i) la ubicación orgánica y vinculación administrativa instrumental de la Superintendencia, sin crear una sexta rama del Poder Público; (ii) el diseño de selección, mandato, remoción y rendición de cuentas; (iii) la tabla de sistemas estatales y leyes habilitantes; (iv) la transición de tratamientos biométricos laborales; (v) las cuantías sancionadoras y prescripción; (vi) las concordancias procesales y jurisprudenciales; y (vii) el calendario de instalación, Registro, auditorías, reglamentos, adecuación y sanciones.

3. Destinatarios y alcance de la consulta

Se propone someter esta versión a consulta, de forma diferenciada, a la mesa de trabajo presidida por Dinorah Figuera, vinculada a la Asamblea Nacional electa en 2015; y a la Presidencia y equipos técnicos y jurídicos de la Asamblea Nacional instalada en enero de 2026 tras las elecciones parlamentarias de 2025, presidida por Jorge Rodríguez para el período 2026-2027. También se invita a colegios de abogados, facultades de Derecho, universidades, colegios profesionales, equipos técnicos y jurídicos de partidos políticos y del entorno de María Corina Machado, especialistas en informática, protección de datos y ciberseguridad, organizaciones de derechos humanos y de la sociedad civil, sectores empresarial y tecnológico y demás personas interesadas. La eventual presentación parlamentaria queda condicionada a la

culminación de la reinstitucionalización democrática y a la constitución de un gobierno elegido democráticamente. La mención de estos destinatarios no implica adhesión, aval, participación en la redacción ni atribución de una posición institucional.

4. Naturaleza jurídica, método y advertencias

La V1.5 es un borrador para consulta y deliberación. El Informe de Adecuación se emplea como insumo técnico de revisión y no como fuente normativa vinculante. Las referencias a la Unión Europea y a España se utilizan como derecho comparado y no atribuyen automáticamente competencias a autoridades venezolanas. Las observaciones que el informe identifica como basadas en memoria o fuentes parciales se señalan como verificaciones pendientes. Antes de la presentación formal será indispensable cotejar el texto vigente de la Constitución, leyes, decretos y Gacetas Oficiales venezolanas, así como completar la revisión constitucional, penal, procesal, administrativa, laboral, registral y de técnica legislativa.

5. Cuestiones que permanecen sometidas a decisión y cotejo

No deben presentarse como hechos jurídicos cerrados, sin decisión legislativa y verificación de fuentes: (a) la ubicación orgánica definitiva de la Superintendencia; (b) el estado actualizado de leyes sectoriales y sistemas estatales; (c) la jurisprudencia vigente del TSJ y las reglas de competencia; (d) las cuantías de multas y prescripción; (e) el alcance final de excepciones biométricas laborales; (f) la calificación orgánica y el procedimiento del artículo 203 constitucional; y (g) los plazos cuya simulación y compatibilidad todavía deban verificarse.

RUTA CONSTITUCIONAL Y LEGISLATIVA (ARTÍCULO 203). Antes de su consignación, el equipo proponente deberá: (i) cerrar el cotejo de fuentes y concordancias; (ii) justificar por escrito el carácter orgánico por desarrollo de derechos constitucionales y marco normativo; (iii) preparar la exposición de motivos, articulado, disposiciones, cuadro comparativo y memoria de impacto institucional, fiscal y tecnológico; (iv) someter el proyecto a la admisión parlamentaria y votación de dos terceras partes de los integrantes presentes cuando corresponda; y (v) remitir, si la Asamblea lo califica de orgánico, a la Sala Constitucional para el control previo previsto en el artículo 203. Esta guía no sustituye el Reglamento Interior y de Debates ni los requisitos que la Asamblea determine al momento de la consignación.

EXPOSICIÓN DE MOTIVOS

I. Necesidad y oportunidad del proyecto

A partir de las fuentes oficiales cotejadas por el equipo redactor para esta versión, no se ha identificado un marco legislativo general que regule de manera sistemática y transversal el tratamiento de datos personales en Venezuela. Esta afirmación deberá volver a verificarse inmediatamente antes de la presentación formal, incluyendo las Gacetas Oficiales y las normas sectoriales o generales que pudieran haberse promulgado o reformado con posterioridad. La Constitución reconoce expresamente, entre otros, el hábeas data y la protección de la vida privada, intimidad, propia imagen y confidencialidad; el proyecto propone desarrollar legislativamente esas garantías.

La necesidad regulatoria no es meramente formal. La transformación digital de la Administración, los servicios financieros, las telecomunicaciones, el empleo, la educación y las plataformas privadas exige reglas previsibles sobre licitud, finalidad, minimización, seguridad, derechos de las personas, supervisión independiente y tutela judicial. La falta de armonización puede generar incertidumbre tanto para los titulares de datos como para los responsables públicos y privados.

II. Anclaje constitucional

La presente Ley se fundamenta principalmente en los artículos 21, 23, 25, 26, 27, 28, 30, 48, 49, 57, 58, 60, 78, 89, 136, 140, 142, 143 y 203 de la Constitución de la República Bolivariana de Venezuela, en cuanto resulten pertinentes a igualdad y no discriminación, tratados de derechos humanos, nulidad de actos lesivos, tutela judicial y amparo constitucional, hábeas data, reparación de víctimas, inviolabilidad de las comunicaciones, debido proceso, libertad de expresión e información, privacidad, derechos de niños, niñas y adolescentes, garantías laborales, organización del Poder Público, institutos autónomos, responsabilidad patrimonial del Estado, acceso a registros administrativos y procedimiento de ley orgánica. El artículo 108 se invoca específicamente para el desarrollo de derechos y competencias vinculados con educación, información y entorno digital, sin convertirlo en el fundamento exclusivo del derecho a la protección de datos.

La acción de hábeas data se reconoce directamente en el artículo 28 constitucional. Toda referencia a criterios jurisprudenciales de la Sala Constitucional se incorporará únicamente después de identificar y cotejar el texto

íntegro, número, fecha y alcance de las decisiones correspondientes; esta versión no atribuye una doctrina concreta a sentencias que no hayan sido verificadas íntegramente.

III. Referentes comparados y estándares internacionales

El diseño considera como parámetros comparados el Reglamento (UE) 2016/679, la Ley Orgánica española 3/2018, la legislación de Ecuador, Brasil y Chile, los Principios Actualizados de la OEA sobre Privacidad y Protección de Datos Personales (2021) y los Estándares Iberoamericanos de Protección de Datos. Los instrumentos internacionales vinculantes para Venezuela se distinguen de las recomendaciones, estándares y demás instrumentos no vinculantes. Cada referencia requiere cotejo de vigencia, ámbito de aplicación y estatus de ratificación antes de su invocación como obligación jurídica.

La experiencia comparada muestra que la autoridad de control necesita independencia real, transparencia en sus nombramientos, presupuesto suficiente y mecanismos de rendición de cuentas. La propuesta evita dar por resuelta la ubicación constitucional de la Superintendencia: su arquitectura deberá armonizarse con la distribución del Poder Público y con las figuras de entes autónomos previstas por la Constitución, sin subordinar las decisiones de supervisión a órganos o sujetos que puedan quedar sometidos a su control.

IV. Alineación con el estándar RGPD

La aproximación al RGPD constituye un parámetro de calidad normativa y de interoperabilidad, no una promesa de reconocimiento automático de adecuación por parte de la Unión Europea. Una eventual evaluación de adecuación dependería de la legislación finalmente aprobada, su aplicación efectiva, la independencia de la autoridad de control, los recursos administrativos y judiciales y las garantías reales de cumplimiento.

V. Arquitectura institucional de la Superintendencia

La V1.5 propone una autoridad pública de control con independencia funcional, técnica, administrativa y financiera, selección abierta, mandato estable, remoción por causas tasadas y control judicial. La forma orgánica de adscripción, integración o autonomía debe ser objeto de análisis constitucional específico a la luz de los artículos 136, 142 y 273 a 274 de la Constitución. La enumeración constitucional de las ramas del Poder Público y las reglas sobre institutos autónomos impiden presentar como pacífica una fórmula de ente situado “fuera de todos los poderes”.

El Consejo Consultivo se concibe como espacio plural y técnico, con representación académica, profesional, social, tecnológica y de sectores regulados. Su función será consultiva y no podrá sustituir las competencias legales de la Superintendencia. Los órganos con funciones de investigación o persecución penal podrán ser convocados como invitados técnicos, sin voto cuando exista conflicto de interés o se debatan asuntos en los que sean sujetos investigados o regulados.

VI. Elementos de vanguardia

La Ley contempla un Registro Nacional de Tratamientos con garantías de integridad, trazabilidad, publicidad limitada y protección desde el diseño. La tecnología de registro distribuido, incluida blockchain, podrá evaluarse como mecanismo técnico opcional, pero no se incorpora como mandato legal ni podrá almacenar datos personales en forma que impida su rectificación o supresión.

VII. Derechos digitales laborales

El Título X desarrolla derechos digitales en el ámbito de las relaciones de trabajo públicas y privadas, con articulación expresa con la legislación laboral, la función pública, la seguridad y salud en el trabajo y las garantías de estabilidad y debido proceso. Su aplicación concreta deberá armonizarse con los estatutos especiales vigentes.

VIII. Régimen general de videovigilancia

El Título XI incorpora un régimen general de videovigilancia y tecnologías de control aplicable a espacios públicos, comerciales, residenciales, colegios y universidades. Aborda expresamente el uso de sistemas de reconocimiento facial y biométrico.

IX. Protección reforzada de los datos biométricos y límites a la identificación automatizada

Los datos biométricos dirigidos a identificar unívocamente a una persona requieren una protección reforzada por la persistencia de las características físicas o conductuales de las que derivan y por los riesgos que pueden producir su pérdida, filtración, reutilización o consulta no autorizada. La reforma distingue entre una imagen ordinaria, que sigue siendo dato personal cuando identifica o hace identificable a una persona, y el dato biométrico resultante de un tratamiento técnico específico dirigido a identificarla o autenticarla de forma unívoca.

La V1.4 establece que el tratamiento biométrico exige, de forma acumulativa, una base de legitimación y una excepción aplicable al tratamiento de categorías especiales. Una relación contractual, laboral, educativa o comercial, la conveniencia tecnológica o la obligación genérica de identificar no constituyen por sí solas habilitación suficiente. Para las autoridades públicas se refuerza la reserva de ley y la delimitación de competencias, finalidades, personas afectadas, datos, plazos, accesos y mecanismos de control.

Se establecen garantías técnicas y organizativas de minimización, separación de registros, cifrado, autenticación reforzada, auditoría, trazabilidad, conservación limitada y destrucción segura. Los proveedores tecnológicos quedan sujetos a instrucciones documentadas y prohibición de reutilización incompatible. Las coincidencias algorítmicas con efectos desfavorables requieren revisión humana y posibilidad de impugnación.

En el ámbito laboral se establece una regla restrictiva frente al fichaje biométrico ordinario. En espacios de acceso público se prohíbe la identificación biométrica remota masiva o indiscriminada, tanto en tiempo real como mediante búsquedas sistemáticas retrospectivas, y se reservan las excepciones policiales a objetivos concretos, supuestos taxativos, habilitación legal especial, necesidad estricta, control independiente, límites temporales y geográficos y trazabilidad.

La regulación toma como parámetros comparados el RGPD, la LOPDGDD, la Ley Orgánica española 7/2021, la Ley Orgánica española 4/2015, el Real Decreto 255/2025 y los Reglamentos (UE) 2025/1208 y 2024/1689. Estas referencias no se trasladan automáticamente al ordenamiento venezolano: corresponde al legislador nacional definir las autoridades y procedimientos propios, con respeto a la Constitución y a las garantías jurisdiccionales. La extensión de la prohibición a búsquedas retrospectivas masivas o exploratorias constituye una opción legislativa de protección reforzada propuesta para Venezuela; no se presenta como una prohibición idéntica y literal del Reglamento europeo de Inteligencia Artificial, cuya regla específica del artículo 5 se refiere a la identificación biométrica remota en tiempo real en espacios de acceso público para fines policiales.

X. Régimen de datos post mortem

La Ley reconoce por primera vez, en el ordenamiento venezolano, un régimen específico para el tratamiento de datos personales de personas fallecidas, con la figura del testamento digital y el mandato a instituciones para la gestión de cuentas y perfiles en línea.

XI. Sistemas de información crediticia

La Ley regula por primera vez en Venezuela, con marco integral, los sistemas de información crediticia y solvencia patrimonial. Establece requisitos estrictos de licitud, plazo máximo de conservación, y articulación con la Superintendencia de las Instituciones del Sector Bancario.

XII. Canales de denuncia interna

La Ley incorpora un régimen específico para los canales de denuncia interna en el sector público y privado, con blindaje del denunciante, confidencialidad reforzada y plazos de conservación tasados.

XIII. Régimen agravado ante brechas con riesgo a la vida

La V1.5 refuerza el régimen de notificación de brechas con riesgo para la vida o la integridad física. La comunicación a la autoridad de control será inmediata; la intervención del Ministerio Público o de autoridades de seguridad deberá responder a una base legal y a la finalidad concreta. Se elimina la notificación automática a órganos de inteligencia, especialmente cuando pueda exponer a víctimas, testigos o personas protegidas. La información al afectado no quedará sometida a una autorización genérica de las autoridades: cualquier diferimiento deberá ser excepcional, temporal, necesario y motivado judicialmente.

XIV. Articulación con la justicia transicional

La Ley prevé un régimen especial reforzado para los datos de víctimas y testigos de la Comisión Nacional de la Verdad, Justicia, Reparación y Sanación, con remisión expresa a su ley orgánica como norma especial prevalente en su ámbito.

XV. Habeas data como capítulo procesal autónomo

La Ley desarrolla el habeas data como capítulo procesal propio, con anclaje directo en el artículo 28 constitucional, dotándolo de procedimiento breve, plazos perentorios y medidas cautelares. Se contempla también la legitimación específica de causahabientes, incluidas las uniones de hecho.

XVI. Ley Orgánica de Ciberseguridad complementaria

La presente Ley preserva su objeto propio: la protección del derecho fundamental a los datos personales. Las infraestructuras críticas y los deberes generales de ciberseguridad podrán ser objeto de una ley complementaria. La disposición transitoria correspondiente formula una propuesta de priorización y coordinación legislativa, sin pretender imponer a la Asamblea Nacional futura la aprobación de una ley en un plazo jurídicamente imperativo.

XVII. Consulta ampliada y ruta de cierre editorial

La V1.5 se somete a consulta técnica, jurídica e institucional ante la mesa de diálogo entre representantes de la Asamblea Nacional del período 2015-2020 y de la Asamblea Nacional del período 2026-2031, así como ante colegios de abogados, facultades de Derecho, universidades, colegios profesionales, equipos técnicos y jurídicos de partidos políticos y del entorno de María Corina Machado, especialistas en informática y ciberseguridad, organizaciones de la sociedad civil y derechos humanos, y sectores empresarial y tecnológico. Se prepara para eventual presentación parlamentaria una vez culminada la reinstitucionalización democrática y constituido un gobierno elegido democráticamente. La mención de destinatarios no implica adhesión, aval, participación en la redacción ni atribución de posición institucional.

XVIII. Estructura de la Ley

La Ley se estructura en catorce Títulos y ciento cuarenta y tres artículos, incluidos los artículos 2 bis, 4 bis, 25 bis y 44 bis; diez Disposiciones Transitorias; una Disposición Derogatoria; y cuatro Disposiciones Finales.

PARTE II

ARTICULADO DE LA V1.5

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto. La presente Ley Orgánica tiene por objeto garantizar el derecho fundamental a la protección de los datos personales y desarrollar, de manera sistemática, las garantías previstas en los artículos 21, 23, 25, 26, 27, 28, 30, 48, 49, 57, 58, 60, 78, 89, 136, 140, 142, 143 y 203 de la Constitución de la República Bolivariana de Venezuela, sin perjuicio de las disposiciones constitucionales especiales aplicables. Regula el tratamiento de datos personales por personas naturales o jurídicas, públicas o privadas, y establece principios, derechos, obligaciones, procedimientos, autoridades de control y mecanismos de tutela. Los artículos 27 y 28 sustentan, respectivamente, la tutela constitucional y el hábeas data; los artículos 25, 30 y 140 se consideran para la nulidad de actuaciones lesivas, la reparación de víctimas y la responsabilidad patrimonial del Estado, dentro de sus respectivos ámbitos. El artículo 108 se desarrolla específicamente en las materias de educación, información y entorno digital.

Artículo 2. Ámbito de aplicación material. Esta Ley se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero o sistema organizado. Se aplica a tratamientos realizados por responsables y encargados

públicos o privados, incluidos los que utilicen algoritmos, inteligencia artificial, elaboración de perfiles, tecnologías biométricas o sistemas de vigilancia, con las exclusiones y salvaguardas específicas previstas en el artículo 2 bis.

Artículo 2 bis. Libertad de expresión, información y actividades personales. La aplicación de esta Ley se interpretará y aplicará de manera compatible con las libertades de expresión e información, el ejercicio del periodismo, la creación literaria, artística y académica, la investigación histórica y el acceso a archivos de interés público. Las solicitudes de supresión, rectificación o desindexación deberán ponderarse, caso por caso, con la veracidad, actualidad, relevancia pública, contexto, interés histórico, derechos de terceros y obligaciones legales de conservación. Esta Ley no podrá utilizarse para imponer censura previa, revelar fuentes periodísticas protegidas ni eliminar de forma automática información de interés público. Lo anterior no exime del deber de rectificar información inexacta, proteger datos de víctimas y menores, ni de observar las garantías de finalidad, seguridad y minimización que resulten compatibles. Queda excluido el tratamiento efectuado por una persona natural en el ejercicio de actividades exclusivamente personales o domésticas, siempre que no se vincule con una actividad profesional, comercial, institucional o de difusión pública.

Artículo 3. Ámbito de aplicación territorial. Esta Ley se aplica al tratamiento de datos personales realizado en el territorio de la República Bolivariana de Venezuela, con independencia del lugar donde se produzcan los hechos que dieron origen al dato o del lugar donde se encuentren los servidores o infraestructuras técnicas del responsable o del encargado, sin perjuicio de lo dispuesto en los artículos 4 y 4 bis.

Artículo 4. Aplicación extraterritorial. Esta Ley se aplica también al tratamiento de datos personales de interesados que se encuentren en Venezuela, realizado por responsables o encargados no establecidos en el país, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados, o con el control de su comportamiento en la medida en que este tenga lugar en el territorio nacional. En tales casos, el responsable o el encargado deberá designar por escrito un representante en Venezuela, conforme a lo previsto en el Título VI de esta Ley.

Artículo 4 bis. Tratamientos efectuados por el Estado venezolano fuera del territorio. Esta Ley se aplica al tratamiento de datos personales efectuado fuera del territorio nacional por órganos y entes del Estado venezolano, incluidas sus misiones diplomáticas y oficinas consulares, cuando actúen en ejercicio de funciones públicas o administrativas de la República. Comprende, entre otros, los tratamientos relacionados con registros consulares, documentos de identidad y viaje, asistencia a nacionales, servicios públicos y expedientes administrativos. Su aplicación no crea por sí sola obligaciones extraterritoriales para responsables privados extranjeros que no estén comprendidos en los criterios del artículo 4 ni en las normas aplicables de derecho internacional.

Artículo 5. Definiciones. A los efectos de esta Ley se entenderá por:

1. Datos personales: toda información sobre una persona natural identificada o identificable.

2. Interesado: la persona natural titular de los datos personales.

3. Tratamiento: toda operación o conjunto de operaciones realizadas sobre datos personales, sean o no automatizadas.

4. Responsable del tratamiento: la persona natural o jurídica, pública o privada, que sola o conjuntamente con otras determine los fines y medios del tratamiento.

5. Encargado del tratamiento: la persona natural o jurídica, pública o privada, que trata datos personales por cuenta del responsable.

6. Consentimiento: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta el tratamiento de sus datos personales.

7. Elaboración de perfiles: toda forma de tratamiento automatizado destinada a evaluar aspectos personales del interesado.

8. Brecha de seguridad: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizado a dichos datos.

9. Brecha de seguridad con riesgo a la vida o la integridad física: aquella brecha de seguridad en la que existan indicios racionales de que los datos personales afectados pueden ser utilizados para atentar contra la integridad física o la vida de personas identificadas o identificables.

10. Autoridad de Control: la Superintendencia Nacional de Protección de Datos Personales creada por esta Ley.

11. Datos ultrasensibles: datos personales cuya pérdida, divulgación, alteración o acceso no autorizado pueda ocasionar un riesgo grave y específico para la vida, integridad, libertad, seguridad, intimidad o ejercicio de derechos fundamentales de una persona, especialmente datos de víctimas, testigos, niños, niñas y adolescentes, personas protegidas y personas expuestas a persecución o violencia. La aplicación de esta categoría se regirá por los supuestos previstos en la Ley; la Superintendencia no podrá crear por vía reglamentaria nuevas categorías sancionables.

12. Sistema de Información de Denuncias Internas: el canal establecido por una entidad pública o privada para la recepción de comunicaciones sobre actos u omisiones que puedan constituir infracciones normativas, contractuales o éticas, dentro de la organización, garantizando la confidencialidad de la identidad del denunciante.

13. Testamento digital: el documento fehaciente por el cual el titular de datos personales dispone, en vida, sobre el destino de sus datos y activos digitales tras su fallecimiento.

14. Videovigilancia: el tratamiento de datos personales realizado a través de sistemas de captación, grabación, transmisión o almacenamiento de imágenes o sonidos, con fines de seguridad, control o registro.

15. Datos biométricos: datos personales obtenidos mediante un tratamiento técnico específico, relativos a características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen su identificación unívoca. Entre ellos pueden encontrarse patrones dactilares, faciales, oculares, de voz, geometría de la mano, marcha u otros rasgos comparables, siempre que el tratamiento permita o confirme dicha identificación.

16. Plantilla biométrica: representación digital derivada de una característica biométrica, generada para efectuar operaciones de identificación o verificación, que permite o puede permitir, por sí sola o en combinación con otros datos, la identificación unívoca de una persona natural.

17. Identificación biométrica: procedimiento técnico automatizado mediante el cual se compara una característica biométrica con una o varias referencias almacenadas, con la finalidad de determinar la identidad de una persona natural o localizar una coincidencia en una base de datos.

18. Verificación o autenticación biométrica: procedimiento técnico automatizado, normalmente uno a uno, mediante el cual se comprueba si una característica biométrica presentada por una persona corresponde a la plantilla previamente asociada a la identidad que esta declara.

19. Reconocimiento facial: tratamiento técnico automatizado de imágenes o representaciones faciales para extraer características y efectuar operaciones de verificación, identificación, clasificación o análisis facial. Su calificación como tratamiento de categoría especial dependerá de que se dirija a identificar unívocamente a una persona, sin perjuicio de las restantes obligaciones de esta Ley.

20. Sistema de identificación biométrica remota: sistema técnico que permite identificar a personas naturales sin su participación activa y, generalmente, a distancia, mediante la comparación de sus datos biométricos con los contenidos en una base de datos de referencia.

21. Identificación biométrica remota en tiempo real: identificación biométrica remota en la que la captura de los datos, su comparación y la identificación se producen sin una demora significativa, incluidas las demoras mínimas que no alteren sustancialmente el carácter inmediato de la operación.

22. Sistema de categorización biométrica: sistema automatizado que clasifica individualmente a personas naturales en categorías a partir de sus datos biométricos. La utilización de estos sistemas quedará sometida a las prohibiciones y garantías establecidas en esta Ley y en la legislación especial aplicable.

23. Anonimización: proceso irreversible, considerando los medios razonablemente disponibles, por el cual los datos dejan de permitir la identificación de una persona natural, directa o indirectamente.

24. Seudonimización: tratamiento por el que los datos no pueden atribuirse a una persona sin utilizar información adicional, conservada separadamente y protegida mediante medidas técnicas y organizativas.

25. Destinatario: persona natural o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, con independencia de que sea tercero.

26. Tercero: persona natural o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o encargado.

27. Autoridad pública: órgano, ente, institución, entidad u organismo que ejerza potestades públicas o funciones administrativas conforme a la Constitución y las leyes.

28. Transferencia internacional: comunicación, transmisión, acceso remoto o puesta a disposición de datos personales a un destinatario situado en otro Estado u organización internacional.

29. Tratamiento a gran escala: tratamiento que, atendiendo al número de interesados, volumen y variedad de datos, duración, extensión geográfica, frecuencia y alcance de las operaciones, pueda producir riesgos elevados para los derechos y libertades.

30. Datos relativos a la salud: datos personales relacionados con la salud física o mental de una persona, incluida la prestación de servicios sanitarios, que revelen información sobre su estado de salud.

31. Datos genéticos: datos personales relativos a características genéticas heredadas o adquiridas que proporcionen información única sobre la fisiología o salud de una persona y que resulten, en particular, del análisis de una muestra biológica.

32. Responsable conjunto: dos o más responsables que determinen conjuntamente los fines y medios del tratamiento y deban distribuir de forma transparente sus responsabilidades conforme a esta Ley.

Artículo 6. Carácter de orden público. Las disposiciones de esta Ley son de orden público. Los derechos que reconoce son irrenunciables. Es nula toda cláusula, pacto o disposición que pretenda excluir, limitar o menoscabar los derechos del interesado.

Artículo 7. Supletoriedad y coordinación normativa. En lo no previsto en esta Ley se aplicarán, según la materia y siempre que sean compatibles con sus principios y garantías, la Ley Orgánica de Procedimientos Administrativos, la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales, la legislación contencioso-administrativa, la legislación procesal laboral, el Código Civil, el Código de Procedimiento Civil, el Código Orgánico Procesal Penal y las demás normas especiales aplicables. La supletoriedad no podrá ampliar potestades sancionadoras, reducir garantías constitucionales ni sustituir las reglas de competencia establecidas en la Constitución y las leyes.

Artículo 8. Interpretación pro persona. En caso de duda sobre la interpretación de esta Ley, se aplicará el criterio más favorable al interesado y a la protección de sus derechos fundamentales. Las excepciones y limitaciones al derecho a la protección de datos personales serán de interpretación restrictiva.

TÍTULO II

PRINCIPIOS RECTORES DEL TRATAMIENTO

Artículo 9. Licitud, lealtad y transparencia. Todo tratamiento de datos personales debe ser lícito, leal y transparente en relación con el interesado. Es lícito el tratamiento realizado con base en alguno de los supuestos de legitimación previstos en el Título III de esta Ley. Es leal el que se realiza sin engaño, sin ocultamiento y sin desviación de la finalidad declarada. Es transparente el que se informa de forma clara, accesible y comprensible al interesado.

Artículo 10. Limitación de la finalidad. Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. El tratamiento ulterior con fines de archivo en interés público, investigación científica o histórica, o fines estadísticos no se considerará incompatible con los fines iniciales, siempre que se apliquen las garantías apropiadas.

Artículo 11. Minimización. Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Ningún tratamiento podrá recolectar más datos que los estrictamente necesarios para la finalidad declarada.

Artículo 12. Exactitud. Los datos personales serán exactos y, cuando sea necesario, actualizados. Se adoptarán todas las medidas razonables para que los datos personales inexactos, en relación con los fines para los que se tratan, sean suprimidos o rectificados sin dilación indebida.

Artículo 13. Limitación del plazo de conservación. Los datos personales serán mantenidos de forma que se permita la identificación del interesado durante no más tiempo del necesario para los fines del tratamiento. El responsable establecerá plazos concretos de conservación o criterios objetivos para determinarlos, y los comunicará al interesado.

Artículo 14. Integridad y confidencialidad. Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.

Artículo 15. Responsabilidad proactiva. El responsable del tratamiento es responsable del cumplimiento de los principios rectores establecidos en este Título y deberá ser capaz de demostrarlo ante la Superintendencia y ante el interesado.

Artículo 16. Protección desde el diseño y por defecto. El responsable aplicará, tanto en el momento de determinar los medios del tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas destinadas a aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

TÍTULO III

BASES DE LEGITIMACIÓN DEL TRATAMIENTO

Artículo 17. Bases de legitimación. El tratamiento de datos personales solo será lícito si concurre al menos una de las siguientes condiciones: 1. El consentimiento del interesado para uno o varios fines específicos. 2. El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. 3. El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable. 4. El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona natural. 5. El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable. 6. El tratamiento es necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.

Artículo 18. Consentimiento. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. El consentimiento deberá ser libre, específico, informado e inequívoco, mediante una declaración o una clara acción afirmativa.

Artículo 19. Tratamiento de datos de niños, niñas y adolescentes. El tratamiento de datos personales de niños, niñas y adolescentes se regirá por el interés superior, la autonomía progresiva, el derecho a ser oído, la edad, madurez y capacidad concreta de comprensión, y las reglas de patria potestad, representación legal y responsabilidad de crianza previstas en la Constitución y la LOPNNA. El responsable documentará, atendiendo a la naturaleza del dato, la finalidad, el riesgo y el contexto, si el niño, niña o adolescente comprende razonablemente el tratamiento y qué intervención corresponde a quienes ejerzan la patria potestad o representación. Cuando la legislación exija consentimiento de dichas personas, este deberá obtenerse sin sustituir el derecho del niño, niña o adolescente a recibir información comprensible y a expresar su opinión conforme a su desarrollo. No se establece un umbral autónomo de catorce años ni se presume una incapacidad uniforme por el solo hecho de ser menor de dieciocho. Los tratamientos de categorías especiales, biométricos, de perfilado o de alto riesgo requerirán habilitación legal y garantías reforzadas; el consentimiento de un representante no podrá subsanar la falta de base jurídica ni autorizar un tratamiento prohibido, y se recabará el asentimiento del menor cuando su edad y madurez permitan una comprensión suficiente.

Artículo 20. Ejecución contractual y demás bases. El tratamiento fundado en la ejecución de un contrato se limitará estrictamente a los datos necesarios para su ejecución o para aplicar, a petición del interesado, medidas precontractuales. El tratamiento fundado en obligación legal o misión de interés público requerirá una norma con rango de ley que determine, con suficiente precisión, la finalidad, los datos o categorías de datos, los sujetos habilitados, las condiciones de acceso, el plazo de conservación y las garantías aplicables. Un acto administrativo podrá ejecutar o concretar una habilitación legal previa, pero no crear por sí mismo una nueva base de legitimación ni ampliar sus elementos esenciales. La protección de intereses vitales se limitará a lo estrictamente necesario y se documentará.

Artículo 21. Interés legítimo. El responsable que pretenda tratar datos personales con base en su interés legítimo o en el de un tercero deberá realizar una ponderación previa y documentada entre dicho interés y los derechos y libertades fundamentales del interesado. El interés legítimo no será base válida para el tratamiento realizado por autoridades públicas en el ejercicio de sus funciones.

Artículo 22. Revocación del consentimiento. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basado en el consentimiento previo a su retirada. Será tan fácil retirar el consentimiento como darlo.

TÍTULO IV

CATEGORÍAS ESPECIALES DE DATOS

Artículo 23. Categorías especiales de datos. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona natural, salvo que concurra alguna de las excepciones taxativamente previstas en esta Ley.

La captación, reproducción o conservación de una fotografía o imagen facial no la convierte automáticamente en dato biométrico de categoría especial. Tendrá tal condición cuando sea sometida a un tratamiento técnico específico dirigido a identificar unívocamente a una persona, sin perjuicio de que la imagen constituya dato personal y quede sometida a las restantes disposiciones de esta Ley.

Artículo 24. Excepciones al tratamiento de categorías especiales.

1. El interesado haya prestado consentimiento explícito, libre, específico, informado e inequívoco para una o varias finalidades determinadas, siempre que dicho consentimiento pueda retirarse con la misma facilidad con la que fue otorgado y que no exista una situación de desequilibrio que impida considerarlo libre.

2. El tratamiento sea necesario para el cumplimiento de obligaciones o el ejercicio de derechos específicos del responsable o del interesado en el ámbito laboral, de seguridad social o de protección social, en la medida en que esté autorizado por una norma con rango de ley que establezca garantías adecuadas y específicas para los derechos de los interesados.

3. El tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona natural, cuando el interesado no esté física o jurídicamente capacitado para prestar su consentimiento y el tratamiento se limite a lo estrictamente necesario para esa protección.

4. El tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos por una actuación propia, consciente e inequívoca, sin que esa circunstancia autorice por sí sola su reutilización para finalidades incompatibles o para la elaboración de perfiles no informados.

5. El tratamiento se realice, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, asociación u otro organismo sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o antiguos miembros o a personas que mantengan contactos regulares con ella en relación con sus fines, y que los datos no se comuniquen fuera de dicha organización sin el consentimiento del interesado.

6. El tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, o cuando los órganos jurisdiccionales actúen en ejercicio de su función judicial, con limitación de los datos a los estrictamente necesarios.

7. El tratamiento sea necesario por razones de interés público esencial, sobre la base de una norma con rango de ley que defina de manera precisa la finalidad, los datos, los sujetos habilitados, las condiciones de acceso, los plazos de conservación y las medidas específicas para salvaguardar los derechos fundamentales, respetando el contenido esencial del derecho a la protección de datos.

8. El tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral, diagnóstico, prestación de asistencia o tratamiento sanitario o social, o gestión de sistemas y servicios de salud, cuando lo permita la legislación aplicable y se encuentre sometido al deber de secreto profesional y a las garantías correspondientes.

9. El tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, sobre la base de una norma con rango de ley que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, incluido el secreto profesional.

10. El tratamiento sea necesario con fines de archivo en interés público, investigación científica o histórica o fines estadísticos, sobre la base de una norma con rango de ley, con respeto al principio de minimización y con garantías técnicas y organizativas adecuadas.

11. El tratamiento de datos biométricos dirigidos a identificar unívocamente a una persona requerirá, de manera acumulativa, una base de legitimación prevista en el artículo 17 y una de las excepciones establecidas en este artículo. La evaluación de impacto, la seguridad reforzada o la autorización administrativa no sustituirán ninguno de esos requisitos.

12. La existencia de una relación contractual, laboral, educativa, comercial, asociativa o de prestación de servicios, así como la conveniencia, rapidez, ahorro de costes o facilidad operativa, no constituirá por sí sola habilitación suficiente para exigir o tratar datos biométricos.

13. El consentimiento explícito no se considerará libre cuando el interesado carezca de una alternativa real, equivalente, accesible y no discriminatoria, o cuando su negativa pueda producir consecuencias desfavorables desproporcionadas. Esta regla se aplicará con especial rigor en relaciones laborales, educativas, sanitarias, de dependencia, de prestación de servicios esenciales y frente a autoridades públicas.

14. Todo tratamiento biométrico realizado por una autoridad pública en ejercicio de potestades de seguridad, investigación penal, control fronterizo, identificación civil, expedición de documentos de identidad o viaje, registro civil, gestión electoral, servicios consulares, prestaciones públicas o potestades administrativas deberá estar previsto en una norma con rango de ley que determine la autoridad competente, la finalidad concreta, las categorías de personas y datos, las condiciones de obtención, acceso, comunicación y conservación, los mecanismos de control y los derechos de los interesados. La autonomía constitucional de las autoridades electorales y de otros órganos no excluye la aplicación de los principios y derechos de protección de datos, pero exige reglas de coordinación que no invadan sus competencias propias.

15. La invocación de interés público esencial no podrá fundarse exclusivamente en referencias genéricas a la seguridad del Estado, seguridad ciudadana, orden público, eficiencia administrativa o interés nacional. La ley habilitante deberá justificar la necesidad y delimitar el alcance material, personal, temporal y territorial del tratamiento.

16. Cuando el tratamiento biométrico sea efectuado por cuenta de una autoridad o entidad responsable mediante un proveedor tecnológico, dicho proveedor actuará bajo instrucciones documentadas, no podrá reutilizar los datos para fines propios ni incorporarlos a bases de datos propias, y quedará sujeto a las obligaciones de confidencialidad, seguridad, auditoría y supresión previstas en esta Ley.

Artículo 25. Datos biométricos y genéticos. El tratamiento de datos biométricos y genéticos requerirá evaluación previa de impacto en la protección de datos y aplicación de medidas técnicas reforzadas. Los datos biométricos utilizados exclusivamente para fines de identificación en el marco de una relación laboral requerirán, además, el cumplimiento de lo dispuesto en el Título X de esta Ley. Los datos genéticos no podrán ser utilizados para fines discriminatorios en el acceso al empleo, a los seguros o a los servicios financieros.

Artículo 25 bis. Garantías especiales del tratamiento biométrico.

1. Todo tratamiento de datos biométricos dirigido a la identificación o autenticación unívoca de una persona estará sometido a los principios de legalidad, finalidad determinada, estricta necesidad, idoneidad, proporcionalidad, minimización, limitación de conservación y responsabilidad proactiva.

2. Antes de implantar el tratamiento, el responsable deberá documentar por qué la finalidad no puede alcanzarse razonablemente con un medio menos intrusivo, igualmente eficaz y accesible, y por qué la operación biométrica resulta necesaria para el supuesto concreto.

3. La evaluación de impacto prevista en los artículos 25 y 47 incluirá, como mínimo: descripción del flujo de captura y comparación; categorías de personas afectadas; finalidad y base jurídica; alternativas no biométricas; análisis de falsos positivos y falsos negativos; rendimiento diferencial entre grupos pertinentes; riesgos de suplantación, inversión o reconstrucción de plantillas; destinatarios y transferencias; plazo de conservación; medidas de mitigación; y mecanismos de revisión humana y reclamación.

4. Los datos biométricos y sus plantillas deberán mantenerse separados de otros registros cuando ello sea técnicamente viable, cifrados en tránsito y en reposo, sometidos a controles de acceso individualizados, autenticación reforzada, registro de consultas y auditorías periódicas. El responsable deberá evaluar el uso de plantillas cancelables, cifrado especializado, procesamiento local o técnicas equivalentes que reduzcan la exposición del rasgo biométrico original.

5. La captura y conservación de muestras biométricas originales solo se permitirá cuando sea estrictamente necesaria y se encuentre expresamente justificada. Cuando la finalidad pueda alcanzarse mediante una plantilla protegida, se evitará conservar la imagen, grabación o muestra original.

6. La creación o mantenimiento de bases de datos biométricas centralizadas por organismos públicos o entidades privadas requerirá habilitación expresa mediante norma con rango de ley. La norma especificará finalidad, categorías

de datos, responsables, sujetos habilitados, criterios de inclusión y exclusión, interoperabilidad permitida y prohibida, plazo de conservación, supresión, auditoría, control independiente y vías de impugnación. La habilitación no se presume por la existencia histórica del sistema, por una competencia genérica de identificación ni por la mera disponibilidad de infraestructura tecnológica.

7. Queda prohibida la reutilización de datos o plantillas biométricas para una finalidad incompatible con aquella que justificó su obtención. Toda finalidad ulterior requerirá nueva habilitación conforme a los artículos 17 y 24 y una evaluación de compatibilidad y riesgos.

8. Los datos biométricos se suprimirán o destruirán de forma segura cuando desaparezca la finalidad o expire la habilitación legal que justificó su tratamiento, salvo obligación legal de conservación que sea específica, necesaria, proporcionada y de duración determinada. Toda excepción deberá quedar documentada y ser revisable.

9. El responsable conservará un registro de cada acceso, consulta, comparación, comunicación, exportación, modificación y supresión de datos biométricos, identificando al usuario, fecha, finalidad, sistema y resultado de la operación. Dichos registros estarán disponibles para la Superintendencia y, cuando proceda, para la autoridad judicial competente.

10. La contratación de proveedores tecnológicos no trasladará ni reducirá la responsabilidad del responsable del tratamiento. El proveedor no podrá crear conjuntos de datos propios, entrenar modelos, realizar pruebas o mejorar productos con datos biométricos del responsable, salvo habilitación autónoma, específica y compatible con esta Ley.

11. Cuando una operación biométrica produzca una coincidencia que pueda generar consecuencias desfavorables para una persona, el resultado deberá ser objeto de comprobación humana por personal capacitado mediante fuentes o procedimientos adicionales. La coincidencia algorítmica no constituirá por sí sola prueba suficiente de identidad o participación en un hecho ilícito.

12. El responsable dispondrá de un procedimiento para que el interesado pueda cuestionar la exactitud de una coincidencia, solicitar revisión humana, conocer la finalidad y los destinatarios del tratamiento y ejercer los derechos reconocidos en esta Ley, con las limitaciones legales estrictamente necesarias en investigaciones en curso.

Artículo 26. Datos de niños, niñas y adolescentes. Los datos personales de niños, niñas y adolescentes merecen una protección específica, en particular en el uso de datos personales con fines de mercadotecnia o elaboración de perfiles. Todo tratamiento se realizará conforme al principio del interés superior consagrado en la Constitución y en la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes.

Artículo 27. Datos relativos a condenas e infracciones. El tratamiento de datos personales relativos a condenas e infracciones penales, o a medidas de seguridad conexas, solo podrá llevarse a cabo bajo la supervisión de las autoridades públicas competentes o cuando lo autorice una norma con rango de ley que establezca las garantías adecuadas para los derechos y libertades de los interesados.

Artículo 28. Datos de víctimas y testigos de justicia transicional. Los datos personales de víctimas, testigos, colaboradores eficaces y personas comparecientes ante la Comisión Nacional de la Verdad, Justicia, Reparación y Sanación tendrán la consideración de datos ultrasensibles y gozarán del estándar de protección más alto previsto en esta Ley. Su tratamiento se regirá por la Ley Orgánica de la Comisión como norma especial prevalente en su ámbito, sin perjuicio de la aplicación supletoria de esta Ley. La Superintendencia Nacional de Protección de Datos Personales conservará la tutela del derecho fundamental una vez extinguida la Comisión.

Artículo 29. Datos ultrasensibles y estándar reforzado. Además de las categorías especiales previstas en los artículos 23 y 28, tendrán consideración de datos ultrasensibles aquellos cuya divulgación, pérdida, alteración o tratamiento ilícito pueda ocasionar un daño grave o irreversible a la persona, en particular cuando se relacionen con víctimas, testigos, personas protegidas, niños, niñas y adolescentes, persecución política, violencia de género o vulnerabilidad extrema. La calificación y sus efectos deberán estar definidos por esta Ley o por una reforma legal. La Superintendencia podrá proponer a la Asamblea Nacional la incorporación de nuevas categorías mediante iniciativa o informe técnico y podrá emitir orientaciones de seguridad, pero no crear nuevas categorías sancionables por reglamento.

Artículo 30. Datos de personas fallecidas. El tratamiento de datos personales de una persona fallecida se regirá por la voluntad del titular expresada en vida mediante documento fehaciente, incluido el testamento digital. A falta de instrucción expresa, las personas vinculadas al fallecido por razones familiares o de hecho, incluidas las uniones estables de hecho sin distinción por orientación sexual, así como sus herederos, podrán solicitar al responsable el acceso, la rectificación o la supresión de los datos, salvo prohibición expresa del causante o disposición legal en

contrario. El régimen de sucesión de los datos y activos digitales se coordinará con las disposiciones del Código Civil en materia de sucesiones. Reglamentariamente se establecerá el desarrollo del testamento digital como instrumento fehaciente.

Artículo 31. Mandato a instituciones para gestión de cuentas y perfiles en línea. El titular podrá designar, en vida, a personas naturales o jurídicas para que gestionen, después de su fallecimiento, sus cuentas, perfiles, activos digitales y contenidos alojados en servicios de la sociedad de la información. La designación se hará mediante testamento digital o instrumento fehaciente equivalente, y podrá incluir instrucciones específicas sobre el destino de cada cuenta, perfil o conjunto de datos. En ausencia de designación, la gestión corresponderá a los causahabientes en los términos del artículo anterior.

Artículo 32. Sistemas de información crediticia y solvencia patrimonial. El tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias solo será lícito cuando los datos sean veraces, la deuda sea cierta, vencida y exigible, y se haya requerido previamente el pago al deudor. Estos datos no podrán mantenerse en los sistemas de información crediticia por un período superior a cinco años contados desde la fecha de vencimiento de la obligación. El interesado tendrá derecho a exigir el registro inmediato del pago cuando este se produzca, y a que no se reincorpore la información una vez transcurrido el plazo. Los sistemas de información crediticia se coordinarán con la Superintendencia de las Instituciones del Sector Bancario, sin perjuicio de la competencia de la Superintendencia Nacional de Protección de Datos Personales en materia del derecho fundamental. El régimen sancionador previsto en el Título XIV de esta Ley se aplicará con carácter reforzado a las entidades que mantengan datos crediticios erróneos, desactualizados o inexactos.

TÍTULO V

DERECHOS DEL INTERESADO

Artículo 33. Derecho de información. El interesado tendrá derecho a recibir del responsable, en el momento de la recogida de los datos, información clara, accesible y comprensible sobre: la identidad y los datos de contacto del responsable y, en su caso, del delegado de protección de datos; los fines del tratamiento y su base jurídica; los destinatarios o categorías de destinatarios; la previsión de transferencias internacionales; el plazo de conservación o los criterios para determinarlo; los derechos que le asisten y la forma de ejercerlos; el derecho a presentar reclamación ante la Superintendencia; la existencia, en su caso, de decisiones automatizadas y elaboración de perfiles.

Artículo 34. Derecho de acceso. El interesado tendrá derecho a obtener del responsable confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la información sobre los fines del tratamiento, las categorías de datos, los destinatarios, el plazo de conservación, y los derechos que le asisten.

Artículo 35. Derecho de rectificación. El interesado tendrá derecho a obtener sin dilación indebida del responsable la rectificación de los datos personales inexactos que le conciernan.

Artículo 36. Derecho de supresión. El interesado tendrá derecho a obtener sin dilación indebida la supresión de los datos personales que le conciernan cuando: 1. Los datos ya no sean necesarios para los fines para los que fueron recogidos. 2. Retire el consentimiento y no exista otra base jurídica. 3. Se oponga al tratamiento y no prevalezcan motivos legítimos imperiosos. 4. Los datos hayan sido tratados ilícitamente. 5. Deban suprimirse para cumplir una obligación legal. El derecho de supresión se ponderará con las obligaciones legales de conservación, la formulación, ejercicio o defensa de reclamaciones, la libertad de expresión e información, el periodismo, los archivos de interés público, la investigación científica, académica o histórica y la protección de derechos de terceros. La limitación o denegación deberá ser específica, motivada, temporal cuando proceda y susceptible de reclamación o revisión judicial. La conservación excepcional no autoriza usos incompatibles.

Artículo 37. Derecho de oposición. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que los datos personales que le conciernan sean objeto de un tratamiento basado en el interés legítimo o en la misión de interés público. Cuando el tratamiento tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse sin necesidad de motivación alguna.

Artículo 38. Derecho de limitación del tratamiento. El interesado tendrá derecho a obtener del responsable la limitación del tratamiento cuando: 1. Impugne la exactitud de los datos. 2. El tratamiento sea ilícito y el interesado se oponga a la supresión. 3. El responsable ya no necesite los datos, pero el interesado los necesite para la

formulación, el ejercicio o la defensa de reclamaciones. 4. El interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen.

Artículo 39. Derecho de portabilidad. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable sin que lo impida el responsable al que se los hubiera facilitado.

Artículo 40. Derecho a no ser objeto de decisiones exclusivamente automatizadas. El interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Artículo 41. Derecho de explicación algorítmica. Cuando el interesado sea objeto de una decisión adoptada total o parcialmente sobre la base de un tratamiento automatizado, incluida la elaboración de perfiles, tendrá derecho a obtener del responsable una explicación clara y comprensible sobre la lógica utilizada, los criterios aplicados, los datos que fueron considerados y las consecuencias previstas del tratamiento.

Artículo 42. Régimen de los canales de denuncia interna. Será lícito el tratamiento de datos personales en el marco de los sistemas de información de denuncias internas, establecidos por entidades públicas o privadas para la recepción de comunicaciones sobre actos u omisiones que puedan constituir infracciones normativas, contractuales o éticas, siempre que se garantice la absoluta confidencialidad de la identidad del denunciante y de las personas investigadas. Las denuncias podrán presentarse de forma anónima, con mecanismos técnicos que preserven la trazabilidad interna sin comprometer el anonimato del denunciante. El acceso a los datos se restringirá al personal responsable de la investigación y, en su caso, a la autoridad competente. Los datos deberán ser suprimidos del sistema transcurridos tres meses desde la recepción de la denuncia, salvo que la finalidad de la conservación sea continuar la investigación judicial, administrativa o disciplinaria. Queda prohibida toda represalia contra el denunciante. El denunciado tendrá derecho a ser informado de la existencia de la denuncia y de su contenido esencial cuando ello no comprometa la investigación.

Artículo 43. Ejercicio y plazos. Los derechos reconocidos en este Título se ejercerán ante el responsable del tratamiento, sin necesidad de intervención de abogado ni de formalidad especial, por cualquier medio que permita acreditar la identidad del interesado. El responsable deberá responder motivadamente en el plazo máximo de veinte días hábiles, prorrogables por otros veinte cuando la complejidad o el volumen de las solicitudes lo justifique.

Artículo 44. Gratuidad y excepciones. El ejercicio de los derechos reconocidos en este Título será gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, el responsable podrá cobrar un canon razonable en función de los costos administrativos, o negarse a actuar, debiendo demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

Artículo 44 bis. Responsabilidad civil y reparación de daños. Toda persona que sufra un daño patrimonial o moral como consecuencia de un tratamiento de datos personales contrario a esta Ley podrá reclamar reparación conforme a las reglas de responsabilidad civil aplicables. Cuando el daño sea imputable al funcionamiento de la Administración Pública, se aplicará además el régimen de responsabilidad patrimonial del Estado previsto en el artículo 140 constitucional, sin perjuicio del artículo 30 cuando se trate de víctimas de violaciones de derechos humanos imputables al Estado. La pretensión deberá acreditar el daño y su relación causal con el incumplimiento, sin perjuicio de las presunciones que establezca expresamente la legislación. Cuando intervengan varios responsables o encargados, la responsabilidad y el eventual régimen de solidaridad se determinarán conforme a su participación, control efectivo del tratamiento y a las normas civiles aplicables. La reparación será independiente de las sanciones administrativas y de las responsabilidades penales que, en su caso, procedan.

TÍTULO VI

OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO

Artículo 45. Deber general de cumplimiento. El responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas naturales, a fin de garantizar y poder demostrar que el tratamiento es conforme con esta Ley.

Artículo 46. Registro de actividades de tratamiento. Todo responsable llevará un registro interno de las actividades de tratamiento efectuadas bajo su responsabilidad. El registro contendrá, como mínimo: nombre y datos de contacto del responsable y, en su caso, del delegado; los fines del tratamiento; una descripción de las categorías

de interesados y de datos; las categorías de destinatarios; las transferencias internacionales previstas; los plazos de conservación; y una descripción general de las medidas técnicas y organizativas de seguridad.

Artículo 47. Evaluación de impacto en la protección de datos. Cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas naturales, el responsable realizará, antes del tratamiento, una evaluación de impacto en la protección de datos. La evaluación será obligatoria en los tratamientos de datos ultrasensibles, en los tratamientos algorítmicos de alto riesgo conforme al Título IX, en los tratamientos que impliquen videovigilancia a gran escala o sistemas de reconocimiento facial y biométrico, y en los tratamientos que impliquen elaboración sistemática de perfiles. Cuando, tras la aplicación de las medidas de mitigación, persista un riesgo alto para los derechos y libertades, el responsable consultará previamente a la Superintendencia y no iniciará el tratamiento hasta cumplir el procedimiento legalmente establecido. En los tratamientos policiales de identificación biométrica remota en espacios de acceso público, la evaluación de impacto en protección de datos se complementará con una evaluación de impacto sobre los derechos fundamentales, sin perjuicio de las autorizaciones y controles exigidos por el artículo 100 y la legislación especial.

Artículo 48. Delegado de protección de datos. El responsable y el encargado designarán un delegado de protección de datos cuando: 1. El tratamiento lo lleve a cabo una autoridad u organismo público. 2. Las actividades principales requieran una observación habitual y sistemática de interesados a gran escala. 3. Las actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos. El delegado no podrá recibir instrucciones respecto al desempeño de sus funciones y no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones.

Artículo 49. Notificación de brechas a la Superintendencia. En caso de brecha de seguridad de datos personales, el responsable la notificará a la Superintendencia sin dilación indebida y, de ser posible, a más tardar en las setenta y dos horas siguientes a que haya tenido constancia de ella. La notificación describirá la naturaleza de la brecha, incluyendo las categorías y el número aproximado de interesados afectados, las categorías y el número aproximado de registros afectados, las posibles consecuencias, y las medidas adoptadas o propuestas por el responsable.

Artículo 50. Régimen agravado de notificación de brechas con riesgo a la vida o la integridad física. Cuando existan indicios racionales de que una brecha de seguridad pueda permitir que los datos afectados se utilicen para atentar contra la vida, integridad física o libertad de personas identificadas o identificables, el responsable: 1. Notificará a la Superintendencia en un plazo no superior a veinticuatro horas desde que tenga constancia, o antes cuando el riesgo requiera respuesta inmediata. 2. Notificará al Ministerio Público cuando existan indicios razonables de la posible comisión de un delito. La comunicación a cuerpos de seguridad u otras autoridades de respuesta urgente solo procederá cuando exista habilitación legal expresa, sea estrictamente necesaria para proteger a las personas y se limite a los datos indispensables. La comunicación a órganos de inteligencia no será automática y requerirá una ley especial aplicable o autorización judicial motivada, con exclusión de identidades de víctimas, testigos y personas protegidas salvo necesidad excepcional y debidamente justificada. 3. Adoptará de inmediato medidas para contener la brecha, mitigar el riesgo y alertar a los interesados afectados. 4. Conservará por cinco años el registro de la brecha, notificaciones y medidas, salvo otro plazo legal específico. Toda comunicación se documentará con identificación del emisor y receptor, fundamento, finalidad, datos comunicados, plazo de conservación y trazabilidad. La aplicación de este artículo no prejuzga responsabilidades penales o civiles.

Artículo 51. Notificación de brechas al interesado. Cuando sea probable que una brecha entrañe un alto riesgo para los derechos y libertades de las personas, el responsable las comunicará sin dilación indebida, en lenguaje claro y sencillo, indicando la naturaleza de la brecha, las consecuencias previsibles y las medidas de protección recomendadas. Si existe riesgo inminente para la vida o la integridad física, la comunicación se realizará de inmediato. Solo podrá diferirse, total o parcialmente, mediante decisión judicial motivada que identifique el riesgo concreto para una investigación en curso, por el tiempo estrictamente necesario y con revisión periódica. La mera solicitud o confirmación administrativa de una autoridad no suspenderá por sí sola el deber de informar.

Artículo 52. Medidas técnicas y organizativas de seguridad. El responsable y el encargado aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluidas, cuando proceda: la seudonimización y el cifrado de los datos personales; la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; la capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida en caso de incidente; y un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas.

Artículo 53. Corresponsabilidad. Cuando dos o más responsables determinen conjuntamente los fines y medios del tratamiento, serán considerados corresponsables. Determinarán, de modo transparente y de común acuerdo, sus respectivas responsabilidades en el cumplimiento de las obligaciones impuestas por esta Ley. El interesado podrá ejercer los derechos que le reconoce esta Ley frente a cada uno de los corresponsables.

Artículo 54. Contrato entre responsable y encargado. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico que lo vincule al responsable, que establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos y las categorías de interesados, y las obligaciones y derechos del responsable.

Artículo 55. Códigos de conducta. Las asociaciones u otros organismos representativos de categorías de responsables o encargados podrán elaborar códigos de conducta destinados a contribuir a la correcta aplicación de esta Ley. Los códigos serán sometidos a la aprobación de la Superintendencia.

Artículo 56. Certificaciones. La Superintendencia promoverá la creación de mecanismos de certificación en materia de protección de datos, así como de sellos y marcas de calidad, con el fin de demostrar el cumplimiento de esta Ley por parte de los responsables y encargados.

Artículo 57. Representación en Venezuela. El responsable o el encargado no establecido en Venezuela, cuando esta Ley les sea aplicable conforme al artículo 4, designará por escrito un representante en el territorio nacional.

Artículo 58. Coordinación con el régimen de ciberseguridad. Las obligaciones establecidas en este Título en materia de seguridad del tratamiento y de notificación de brechas se coordinarán con las obligaciones que en materia de ciberseguridad se establezcan por la Ley Orgánica de Ciberseguridad prevista en la Disposición Transitoria Séptima de esta Ley. La Superintendencia y la autoridad de ciberseguridad que dicha Ley designe establecerán mediante protocolo conjunto los criterios de coordinación, los canales únicos de notificación y las reglas de reparto de competencias sancionadoras, con el fin de evitar duplicación de cargas para los responsables y de garantizar la máxima eficacia de la respuesta institucional ante incidentes.

TÍTULO VII

HABEAS DATA

Artículo 59. Naturaleza y anclaje constitucional. El habeas data es la acción constitucional consagrada en el artículo 28 de la Constitución de la República Bolivariana de Venezuela, mediante la cual toda persona puede acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones legales, así como conocer el uso que se haga de ellos y su finalidad, y solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos datos que sean erróneos o afecten ilegítimamente sus derechos.

Artículo 60. Legitimación activa y pasiva. Están legitimados para ejercer la acción de hábeas data: 1. La persona titular de los datos. 2. Sus padres, madres, representantes legales o apoyos reconocidos por la ley, en nombre de niños, niñas, adolescentes o personas que requieran asistencia. 3. La Defensoría del Pueblo, en el marco de las atribuciones expresamente reconocidas por el artículo 281.3 constitucional. 4. Las personas o entidades que acrediten representación, mandato o afectación de intereses colectivos o difusos, conforme al artículo 26 constitucional y a las reglas legales de representación, legitimación, control judicial y ausencia de conflicto de intereses. Las organizaciones legalmente constituidas podrán actuar cuando su objeto y la afectación concreta justifiquen la representación, sin sustituir automáticamente la voluntad de titulares identificables. Está legitimado pasivamente el responsable y, cuando proceda, el encargado del tratamiento.

Artículo 61. Legitimación de causahabientes y régimen post mortem. Los causahabientes del titular fallecido podrán ejercer la acción de habeas data en relación con los datos personales del difunto, con las siguientes reglas: 1. La legitimación se acreditará mediante el vínculo sucesoral conforme al Código Civil, el reconocimiento de unión estable de hecho conforme a la normativa aplicable, sin distinción por orientación sexual, o cualquier otro instrumento fehaciente. 2. El ejercicio comprenderá tanto los derechos patrimoniales como los morales sobre la identidad digital del difunto. 3. La acción no procederá cuando el causante haya expresado en vida, mediante testamento digital o instrumento fehaciente equivalente, su voluntad contraria al ejercicio de tales derechos por parte de los causahabientes, ni cuando una disposición legal lo prohíba expresamente. 4. En el caso de personas fallecidas de relevancia pública, podrán ejercer la acción, además de los causahabientes, las asociaciones legalmente constituidas cuyo objeto estatutario incluya la defensa de la memoria histórica, la reputación o la dignidad de personas fallecidas, previa acreditación del interés legítimo y de la afectación concreta. Su legitimación no podrá utilizarse para impedir investigaciones periodísticas, académicas o históricas de interés público, ni para suprimir

información veraz sobre hechos de relevancia pública; el tribunal ponderará los derechos en conflicto y ordenará, cuando proceda, rectificación, contextualización, limitación o supresión proporcional. 5. En lo no previsto en este artículo, se aplicará supletoriamente el régimen sustantivo del artículo 30 de esta Ley.

Artículo 62. Competencia y coordinación procesal. La competencia para conocer de la acción de hábeas data se determinará conforme a la Constitución, la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales, la Ley Orgánica del Tribunal Supremo de Justicia, la legislación orgánica del Poder Judicial y las reglas de competencia por materia y territorio vigentes al momento de interposición. En principio conocerá el tribunal de primera instancia cuya competencia material sea afín con la naturaleza del derecho afectado, sin perjuicio de las competencias especiales constitucionales. Esta Ley no crea una categoría de tribunal distinta. La reclamación administrativa ante la Superintendencia no será requisito obligatorio ni impedirá acudir a la tutela judicial; la presentación simultánea se regirá por coordinación, prevención, acumulación o litispendencia conforme a la legislación procesal, evitando decisiones contradictorias sin restringir medidas urgentes. La reforma futura de la Ley Orgánica del TSJ o de la legislación procesal obligará a revisar esta concordancia antes de la consignación parlamentaria

Artículo 63. Procedimiento breve. La acción de habeas data se tramitará por procedimiento breve, oral y expedito, con las siguientes fases: 1. Interpuesta la solicitud, el tribunal la admitirá dentro de las cuarenta y ocho horas siguientes, si cumple los requisitos formales. 2. Admitida la acción, se ordenará la citación del responsable, quien deberá comparecer y contestar dentro de los cinco días hábiles siguientes. 3. Se celebrará audiencia oral dentro de los cinco días hábiles siguientes a la contestación. 4. El tribunal dictará sentencia dentro de los diez días hábiles siguientes a la audiencia. La totalidad del procedimiento no excederá de treinta días hábiles, salvo prórroga motivada por complejidad probatoria.

Artículo 64. Medidas cautelares. En cualquier estado del procedimiento, el tribunal podrá, de oficio o a instancia de parte, decretar medidas cautelares para asegurar la efectividad de la sentencia, incluyendo la suspensión provisional del tratamiento impugnado, la limitación del acceso a los datos, o cualquier otra medida idónea. Las medidas cautelares se decretarán sin necesidad de caución cuando el interesado sea persona natural.

Artículo 65. Sentencia. La sentencia que declare con lugar la acción ordenará al responsable, según corresponda, el acceso a los datos, su rectificación, su supresión, su actualización, la limitación del tratamiento, la cesación del tratamiento ilícito, o cualquier otra medida idónea para el restablecimiento del derecho vulnerado.

Artículo 66. Ejecución. La sentencia definitiva será de ejecución inmediata. En caso de incumplimiento por parte del responsable, el tribunal podrá imponer multas coercitivas diarias, sin perjuicio de la responsabilidad administrativa ante la Superintendencia y de la responsabilidad penal que pudiera corresponder por desacato.

Artículo 67. Apelación, efectos y revisión constitucional. Contra la sentencia definitiva procederá la apelación en los términos y lapsos previstos en la legislación procesal aplicable. La eventual revisión por la Sala Constitucional se regirá por la Constitución, incluido el artículo 336, numeral 10, y la jurisprudencia vinculante vigente. La revisión constitucional no se configura como tercera instancia ni como recurso ordinario de ejercicio automático. Los efectos de la sentencia, su alcance individual, colectivo o difuso, la representación de grupos, la cosa juzgada y la coordinación con procesos conexos se determinarán conforme a la Constitución y las leyes procesales. La presente regulación deberá actualizarse tras cualquier reforma de la Ley Orgánica del TSJ o de la legislación de amparo.

Artículo 68. Articulación con el amparo constitucional. La acción de habeas data no excluye ni sustituye al amparo constitucional. El interesado podrá optar por el habeas data cuando la lesión provenga específicamente del tratamiento de sus datos personales, o por el amparo cuando la lesión afecte otros derechos constitucionales.

Artículo 69. Gratuidad del procedimiento. El procedimiento de hábeas data será gratuito en los términos establecidos por la ley. No se causarán tasas judiciales por la presentación de la acción. La asistencia de abogado no será obligatoria salvo que la ley procesal o la complejidad del caso así lo requieran. La Defensa Pública prestará asistencia jurídica gratuita conforme a su ley orgánica, competencias, organización y disponibilidad presupuestaria, sin perjuicio de la legitimación constitucional de la Defensoría del Pueblo.

TÍTULO VIII

REGISTRO NACIONAL DE TRATAMIENTOS DE DATOS PERSONALES

Artículo 70. Naturaleza y objeto del Registro. Se crea el Registro Nacional de Tratamientos de Datos Personales, administrado por la Superintendencia, como instrumento de transparencia, trazabilidad y supervisión de las actividades de tratamiento sujetas a inscripción conforme al artículo 71. El Registro empleará tecnologías adecuadas para garantizar autenticidad, integridad, disponibilidad, trazabilidad y seguridad. La tecnología de registro distribuido,

incluida blockchain, será opcional y solo podrá emplearse cuando una evaluación técnica y de impacto demuestre su compatibilidad con los derechos de rectificación, supresión, minimización y seguridad.

Artículo 71. Inscripción y régimen diferenciado. Estarán obligados a inscribirse en el Registro Nacional de Tratamientos: 1. Los órganos y entes del sector público. 2. Los responsables y encargados que traten categorías especiales o datos ultrasensibles a gran escala. 3. Quienes realicen tratamientos de alto riesgo o elaboren perfiles sistemáticos con efectos significativos. 4. Las entidades que la Ley identifique expresamente por la naturaleza o volumen de sus operaciones. Las personas naturales que realicen tratamientos exclusivamente personales o domésticos están excluidas. Las microempresas y profesionales independientes podrán acogerse a un régimen simplificado cuando el tratamiento no sea de alto riesgo ni involucre categorías especiales a gran escala. Todo responsable, incluso si no está obligado a inscribirse, mantendrá el registro interno previsto en el artículo 46.

Artículo 72. Contenido mínimo, campos públicos y reserva. La inscripción contendrá, como mínimo: identificación jurídica y datos de contacto del responsable; finalidades; bases de legitimación; categorías generales de datos e interesados; destinatarios o categorías de destinatarios; transferencias internacionales; plazos generales de conservación; medidas generales de seguridad; delegado de protección de datos cuando corresponda; y evaluación de impacto en los supuestos legalmente previstos. La Superintendencia definirá por norma técnica subordinada a la Ley los campos de acceso público y los campos reservados, aplicando minimización, seguridad, secreto legal y prevención de reidentificación. La consulta pública no revelará datos personales, secretos comerciales, vulnerabilidades técnicas, credenciales, detalles operativos de seguridad ni información cuya divulgación comprometa derechos o funciones constitucionales.

En ningún caso se incorporarán al Registro Nacional de Tratamientos de acceso público plantillas biométricas, imágenes faciales destinadas a identificación, impresiones dactilares, muestras genéticas ni identificadores que permitan reconstruir, localizar o vincular esos datos con una persona natural. La información pública se limitará a metadatos no identificativos del tratamiento. La Superintendencia tendrá acceso a la información completa que resulte necesaria para el ejercicio de sus competencias, bajo deber de reserva y controles de acceso.

Artículo 73. Integridad y trazabilidad tecnológica del Registro. El Registro utilizará mecanismos fiables de integridad, autenticidad, sello de tiempo y trazabilidad, mediante tecnología apropiada y tecnológicamente neutral. La tecnología de registro distribuido o blockchain podrá emplearse como opción, previa evaluación de impacto y seguridad, pero no será obligatoria. Los datos personales, documentos y asientos descriptivos que deban rectificarse o suprimirse se conservarán fuera de cualquier estructura inmutable; en un registro distribuido solo podrán incorporarse huellas criptográficas generadas mediante técnicas que impidan razonablemente la reversión o reidentificación, sin datos identificativos directos, metadatos excesivos ni hashes simples de identificadores personales. La arquitectura deberá someterse a pruebas independientes de reidentificación, gestión segura de claves y auditorías periódicas. Toda modificación, rectificación o supresión deberá quedar trazable y ser jurídicamente efectiva.

Artículo 74. Publicidad, acceso y verificación ciudadana. El Registro será de acceso público y gratuito respecto de los campos expresamente declarados públicos por esta Ley y por sus normas de desarrollo. El interesado tendrá acceso completo a los datos relativos a sus tratamientos, salvo limitaciones legales estrictas y motivadas. La consulta pública no incluirá detalles técnicos de seguridad, datos personales de contacto no destinados a publicidad, ni otra información reservada. La Superintendencia ofrecerá mecanismos de verificación de integridad y una vía de reclamación para corregir datos inexactos.

Artículo 75. Régimen transitorio de implementación. La implementación del Registro se realizará por fases, conforme a las prioridades, plazos y categorías de responsables establecidas en los artículos 71 a 74 y en la Disposición Transitoria Tercera. La Superintendencia publicará el calendario, los requisitos y las especificaciones técnicas previa consulta pública. La implementación no dependerá de una tecnología determinada ni exigirá la incorporación de datos personales a estructuras inmutables.

TÍTULO IX

GOBERNANZA ALGORÍTMICA E INTELIGENCIA ARTIFICIAL

Artículo 76. Ámbito de aplicación. Este Título se aplica a todo tratamiento automatizado de datos personales que utilice sistemas algorítmicos, técnicas de aprendizaje automático, inteligencia artificial o cualquier tecnología análoga, y que produzca efectos jurídicos en el interesado o le afecte significativamente.

Artículo 77. Transparencia algorítmica. El responsable que utilice sistemas algorítmicos deberá informar al interesado, en lenguaje claro y comprensible, sobre: la existencia del tratamiento algorítmico; la finalidad y la lógica general aplicada; las categorías de datos utilizadas como insumo; las consecuencias previstas del tratamiento; y los derechos que le asisten conforme a esta Ley.

Artículo 78. Derecho a explicación humana. Cuando el interesado sea objeto de una decisión automatizada o semiautomatizada, tendrá derecho a solicitar la intervención humana por parte del responsable, a expresar su punto de vista, a obtener una explicación de la decisión y a impugnarla. La intervención humana deberá ser sustantiva y no meramente formal.

Artículo 79. Evaluación de impacto algorítmico. Toda entrada en funcionamiento de un sistema algorítmico de alto riesgo requerirá evaluación previa de impacto en la protección de datos, que incluirá: descripción del sistema y de la lógica aplicada; análisis de proporcionalidad; identificación de riesgos para los derechos y libertades; medidas de mitigación; mecanismos de auditoría; y evaluación de sesgos discriminatorios.

Artículo 80. Tratamientos de alto riesgo. Se consideran tratamientos algorítmicos de alto riesgo aquellos que se refieran a: evaluación o clasificación crediticia; selección, evaluación o desvinculación laboral; acceso a servicios esenciales; determinación de riesgo en materia de seguros; evaluación de estudiantes y candidatos a estudios; identificación biométrica en espacios de acceso público; identificación biométrica remota en tiempo real o retrospectiva; cotejos con bases de datos públicas o policiales; categorización biométrica; tratamiento biométrico a gran escala de niños, niñas y adolescentes; inferencia de emociones; decisiones de riesgo penal, migratorio, laboral o educativo basadas en biometría; y elegibilidad para prestaciones sociales. La Superintendencia podrá evaluar otros tratamientos conforme a criterios legales objetivos de escala, finalidad, efectos y riesgo, sin crear por vía reglamentaria prohibiciones, excepciones materiales, categorías sancionables ni habilitaciones no previstas por ley. La clasificación como alto riesgo no autoriza por sí misma el tratamiento ni sustituye las bases y excepciones exigidas por los artículos 17 y 24.

Artículo 81. Prohibición de decisiones exclusivamente automatizadas en materias sensibles. Queda prohibida la adopción de decisiones basadas exclusivamente en tratamiento automatizado, sin intervención humana efectiva, en las siguientes materias: salud; empleo y relaciones laborales; acceso al crédito y a servicios financieros esenciales; justicia y ejercicio de derechos procesales; elegibilidad para prestaciones sociales; educación en cuanto a decisiones definitivas de admisión, promoción o titulación; y migración y protección internacional.

Artículo 82. Salvaguardas específicas en materias sensibles. En las materias enumeradas en el artículo anterior, además de la intervención humana efectiva, el responsable garantizará: registro pormenorizado de la decisión, incluyendo motivación individualizada; derecho de revisión en un plazo no superior a treinta días; asistencia jurídica gratuita cuando el interesado lo requiera; y prohibición de aplicar decisiones desfavorables mientras esté pendiente la revisión.

Artículo 83. Auditoría algorítmica. La Superintendencia podrá ordenar, de oficio o a instancia de parte, la auditoría técnica de sistemas algorítmicos que traten datos personales. La auditoría podrá versar sobre: cumplimiento de los principios de esta Ley; existencia de sesgos discriminatorios; adecuación de las medidas de mitigación; y correspondencia entre la lógica declarada y la efectivamente aplicada.

Artículo 84. Responsabilidad por sesgo discriminatorio. La utilización de sistemas algorítmicos que produzcan resultados discriminatorios por origen étnico, género, edad, condición social, orientación sexual, discapacidad o cualquier otra categoría protegida constitucionalmente comprometerá la responsabilidad del responsable del tratamiento, con independencia de que el resultado haya sido intencional.

Artículo 85. Certificación de sistemas algorítmicos. La Superintendencia promoverá esquemas de certificación voluntaria para sistemas algorítmicos que traten datos personales. La certificación acreditará el cumplimiento de estándares técnicos y éticos definidos reglamentariamente y podrá considerarse elemento favorable en la graduación de sanciones.

TÍTULO X

DERECHOS DIGITALES LABORALES

Artículo 86. Ámbito y anclaje normativo. Este Título regula la protección de datos personales de trabajadoras y trabajadores en relaciones laborales públicas y privadas, incluidas las relaciones de empleo público y las modalidades de contratación que, conforme a la ley, encubran una relación de trabajo. Se articula con la Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras, la legislación de seguridad y salud en el trabajo, la Ley del Estatuto de la Función Pública y las normas procesales y estatutarias aplicables. La Superintendencia conocerá de la licitud del tratamiento de datos; las autoridades laborales y administrativas conocerán de los efectos sobre la relación de trabajo, con deber de cooperación y remisión de actuaciones.

Artículo 87. Derecho a la desconexión digital. Las trabajadoras y trabajadores tienen derecho a la desconexión digital fuera de la jornada laboral y durante los períodos de descanso, permiso, vacaciones y suspensión de la relación de trabajo. El empleador elaborará, previa consulta con los representantes de los trabajadores, una política interna de desconexión digital.

Artículo 88. Protección de la intimidad frente a dispositivos digitales del empleador. El empleador podrá acceder a contenidos derivados del uso de dispositivos puestos a disposición del trabajador únicamente cuando exista una política escrita, comunicada previamente, que defina finalidades, alcance, medios y garantías; el acceso sea necesario y proporcional para controlar obligaciones laborales concretas o proteger legítimamente los sistemas y bienes; y se respeten la intimidad y la inviolabilidad de las comunicaciones. Se distinguirá entre usos profesionales y personales. Queda prohibido el acceso indiscriminado a cuentas privadas, comunicaciones personales o contenidos ajenos a la finalidad laboral. Cuando resulte posible, la actuación se limitará a los datos estrictamente necesarios y se informará al trabajador o a sus representantes.

Artículo 89. Videovigilancia en el puesto de trabajo. El empleador podrá utilizar videovigilancia solo para finalidades laborales legítimas, determinadas y proporcionales, con información previa y visible a los trabajadores y sus representantes y con evaluación de impacto cuando corresponda. Queda prohibida la grabación de sonido y la videovigilancia en baños, vestuarios, comedores, zonas de descanso o espacios de intimidad. Las imágenes se suprimirán en un plazo máximo de cuarenta y cinco días, salvo conservación estrictamente necesaria para documentar un incidente concreto o atender una obligación legal o reclamación, con acceso restringido, motivación escrita y plazo limitado. Se prohíbe utilizar la videovigilancia para medir de forma continua la productividad, inferir emociones o elaborar perfiles incompatibles.

Artículo 90. Geolocalización laboral. La geolocalización solo podrá tratarse cuando sea necesaria y proporcional para una función laboral concreta, se utilice un vehículo o dispositivo de la empresa o exista otra habilitación legal suficiente, y los trabajadores hayan recibido información previa, clara y documentada. El seguimiento se limitará al horario de trabajo y se desactivará fuera de la jornada, salvo una necesidad excepcional prevista por ley y estrictamente delimitada. Se prohíbe la geolocalización encubierta o permanente de dispositivos personales y se exigirá evaluación de impacto cuando el seguimiento sea sistemático o de alto riesgo.

Artículo 91. Prohibición general y excepciones del uso biométrico laboral.

1. Queda prohibida la utilización ordinaria y generalizada de reconocimiento facial, huellas dactilares, iris, voz u otros identificadores biométricos para registrar jornada, controlar asistencia, verificar presencia habitual o gestionar accesos ordinarios de trabajadores.

2. La obligación legal de registrar la jornada, supervisar obligaciones laborales o proteger instalaciones no constituye, por sí sola, habilitación para tratar datos biométricos.

3. El tratamiento biométrico laboral solo podrá admitirse cuando una ley formal y expresa establezca el supuesto, finalidad, colectivos afectados, datos y garantías; demuestre necesidad estricta y ausencia de alternativa no biométrica igualmente eficaz y accesible; y cumpla acumulativamente los artículos 17, 24, 25 y 25 bis.

4. La habilitación requerirá evaluación de impacto previa, consulta a representantes de trabajadores, información clara, medidas reforzadas, revisión periódica, acceso limitado y conservación determinada. La consulta o negociación colectiva no sustituye la habilitación legal.

5. El consentimiento individual o una cláusula contractual no serán suficientes cuando exista desequilibrio que impida considerarlo libre o cuando la negativa produzca consecuencias desfavorables desproporcionadas.

6. La negativa no dará lugar a sanción, represalia, discriminación, pérdida salarial, modificación perjudicial de condiciones, despido ni denegación de empleo cuando no exista habilitación legal específica. Se ofrecerá alternativa no biométrica equivalente, accesible y no discriminatoria. La obtención o uso de datos biométricos en contravención de este artículo no podrá justificar por sí sola una medida disciplinaria ni constituir prueba lícita determinante en un procedimiento laboral, sin perjuicio de la valoración judicial de cada caso y de las reglas procesales sobre prueba ilícita.

7. No se conservarán muestras biométricas originales cuando la finalidad pueda alcanzarse mediante una plantilla protegida; esta se suprimirá al desaparecer la finalidad o habilitación.

8. Queda prohibida la reutilización para medir productividad, inferir emociones, clasificar comportamientos o elaborar perfiles distintos de los expresamente autorizados por ley.

9. Los sistemas preexistentes no quedan legitimados por su mera existencia y se someterán al inventario, auditoría y régimen transitorio previsto en la Disposición Transitoria Décima. La Superintendencia podrá ordenar medidas correctoras o suspensión cuando, una vez instalada, constate falta de habilitación o garantías.

Artículo 92. Protección frente al management algorítmico. Las trabajadoras y trabajadores tienen derecho a ser informados por el empleador de los parámetros, reglas e instrucciones en los que se basen los algoritmos o sistemas de inteligencia artificial que afecten a la toma de decisiones que puedan incidir en las condiciones de trabajo. Ninguna decisión de despido, sanción disciplinaria, modificación sustancial de condiciones de trabajo o denegación de acceso al empleo podrá fundamentarse exclusivamente en un tratamiento automatizado.

Artículo 93. Evaluación automatizada del desempeño. Los sistemas de evaluación automatizada o semiautomatizada del desempeño laboral deberán ser transparentes en sus parámetros, permitir la contradicción por parte del trabajador, y estar sujetos a auditoría por sesgo.

Artículo 94. Negociación colectiva de derechos digitales. Las materias reguladas en este Título podrán ser objeto de negociación colectiva. Los convenios colectivos podrán establecer garantías adicionales a las previstas en esta Ley, pero no podrán establecer condiciones menos favorables al trabajador.

Artículo 95. Régimen especial del teletrabajo. En el marco del teletrabajo, el derecho a la desconexión digital se garantizará de manera reforzada. El empleador no podrá exigir la instalación de sistemas de vigilancia continua, de captación permanente de imagen o sonido, ni de acceso al domicilio del teletrabajador, salvo con su consentimiento libre y expreso, revocable en cualquier momento.

TÍTULO XI

RÉGIMEN GENERAL DE VIDEOVIGILANCIA Y TECNOLOGÍAS DE CONTROL

Artículo 96. Ámbito y principio de proporcionalidad. Este Título regula el tratamiento de datos personales realizado a través de sistemas de videovigilancia, cámaras de seguridad y tecnologías análogas de control, en espacios públicos, comerciales, residenciales, educativos y cualquier otro no comprendido en el régimen laboral del Título X. Todo tratamiento se regirá estrictamente por el principio de proporcionalidad.

Artículo 97. Información previa visible. El responsable del tratamiento deberá informar de forma visible al ciudadano, mediante señalización clara e inequívoca, sobre la existencia del sistema de videovigilancia, la identidad del responsable, la finalidad del tratamiento, y los derechos que le asisten conforme a esta Ley.

Artículo 98. Prohibiciones y limitaciones. Queda prohibida la instalación de sistemas de videovigilancia y de captación de sonidos en lugares destinados al descanso, la intimidad o el esparcimiento. Queda igualmente prohibida la captación de sonidos en la vía pública, salvo autorización expresa por norma con rango de ley.

Artículo 99. Plazo de conservación. Las imágenes y sonidos captados por sistemas de videovigilancia serán suprimidos en un plazo máximo de treinta días desde su captación, salvo que deban conservarse para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

Artículo 100. Régimen especial de identificación biométrica y reconocimiento facial.

1. La utilización de sistemas de reconocimiento facial o identificación biométrica en espacios de acceso público quedará sometida a los artículos 17, 24, 25, 25 bis, 47 y 80 de esta Ley, así como a las garantías adicionales establecidas en este artículo. La clasificación de un tratamiento como de alto riesgo no constituirá por sí misma autorización para realizarlo.

2. La verificación biométrica individual uno-a-uno, en la que una persona participa activamente para confirmar una identidad previamente declarada, no se equiparará automáticamente a la identificación biométrica remota. En todo caso, requerirá base de legitimación y excepción válidas, necesidad, proporcionalidad, información y alternativa no biométrica cuando el consentimiento no sea libre o el servicio no pueda condicionarse legalmente a la biometría.

3. Queda prohibida la identificación biométrica remota masiva, generalizada o indiscriminada de personas en espacios de acceso público, tanto en tiempo real como mediante búsquedas sistemáticas retrospectivas sobre grabaciones, salvo que una ley orgánica especial establezca una excepción concreta, estrictamente necesaria y sujeta a las garantías de este artículo.

4. La identificación biométrica remota retrospectiva sobre grabaciones ya obtenidas solo podrá utilizarse en una investigación concreta para localizar o verificar a una persona objetivo previamente individualizada con base en hechos objetivos, cuando una ley orgánica especial determine taxativamente los delitos y supuestos habilitantes y

exista autorización judicial previa y motivada. La resolución delimitará la fuente, período, ámbito geográfico, base de comparación, finalidad y responsables. Queda prohibido el cotejo retrospectivo masivo o exploratorio destinado a descubrir identidades, elaborar listas de población o crear perfiles generales.

5. Los organismos de seguridad pública solo podrán utilizar sistemas de identificación biométrica remota en tiempo real para confirmar la identidad de una persona objetivo concreta y previamente individualizada, en los siguientes supuestos tasados: a) búsqueda de una persona desaparecida o de una víctima concreta de secuestro, trata de personas o explotación; b) prevención de una amenaza específica, grave e inminente contra la vida o integridad física de personas, o de un atentado terrorista real y actual o razonablemente previsible; c) localización o identificación de una persona sospechosa de alguno de los delitos graves expresamente enumerados en una ley orgánica especial, cuando existan hechos objetivos y verificables que vinculen a esa persona con la investigación.

6. La habilitación legal especial deberá definir de forma taxativa los delitos y umbrales de gravedad que permitan la operación, las autoridades competentes, el estándar de indicios, las finalidades, las categorías de personas, las bases de comparación autorizadas, los límites territoriales y temporales y el régimen de control. La referencia genérica a “delitos graves”, “seguridad del Estado”, “orden público” o “interés nacional” no será suficiente.

7. Cada operación requerirá autorización judicial previa y motivada del tribunal competente, solicitada por la autoridad legalmente habilitada. La solicitud deberá individualizar la persona objetivo, describir los hechos objetivos que justifican la medida, explicar por qué no existe una alternativa menos intrusiva y delimitar lugar, duración, sistema, base de referencia y responsables de la operación. La autorización no podrá ser genérica, prospectiva ni extenderse a personas no individualizadas.

8. En una situación de urgencia excepcional, concreta y documentada ante un riesgo inminente para la vida o la integridad física, la ley especial podrá prever el inicio provisional de la operación sin autorización previa, siempre que la solicitud de ratificación judicial se presente sin demora y, en todo caso, dentro de las veinticuatro horas siguientes. Si la autorización se deniega o no se solicita en plazo, el uso cesará inmediatamente y se suprimirán los datos obtenidos, sin perjuicio de la conservación estrictamente necesaria de evidencias bajo orden judicial y con base jurídica independiente.

9. Antes de cada sistema y de cada modalidad de despliegue se realizará una evaluación de impacto de protección de datos y una evaluación de impacto sobre los derechos fundamentales. La evaluación examinará, al menos, necesidad, idoneidad, proporcionalidad estricta, tasas de falsos positivos y falsos negativos, sesgos, grupos especialmente vulnerables, riesgos de vigilancia, duración, alcance territorial, personas incidentalmente captadas y vías de impugnación.

10. Los sistemas utilizados deberán estar inscritos en un registro especial de acceso restringido a la Superintendencia y a los órganos de control legalmente habilitados. Se documentarán las solicitudes, autorizaciones, operaciones ejecutadas, funcionarios y proveedores participantes, consultas, coincidencias, revisiones humanas, comunicaciones y destrucciones. La Superintendencia publicará estadísticas agregadas y anonimizadas, sin revelar información operativa sensible.

11. El resultado de una coincidencia biométrica no podrá constituir por sí solo fundamento para detener, imputar, sancionar, denegar un derecho o adoptar otra decisión desfavorable. Será obligatoria la verificación humana por personal capacitado y la corroboración mediante elementos independientes. La persona afectada tendrá derecho a impugnar la identificación, con las limitaciones temporales y de acceso que sean necesarias y estén motivadas para proteger una investigación en curso.

12. Los datos de personas que no sean el objetivo de la operación y que hayan sido captados incidentalmente deberán suprimirse sin dilación cuando no exista una habilitación legal independiente, específica y documentada para conservarlos. La conservación excepcional deberá quedar motivada, limitada y sometida a revisión judicial o de la autoridad de control.

13. Queda prohibida la creación o ampliación de bases de datos de reconocimiento facial mediante extracción indiscriminada de imágenes de Internet, redes sociales, videovigilancia u otras fuentes públicas o privadas. También quedan prohibidas la categorización biométrica para inferir características sensibles y la inferencia de emociones en los ámbitos laboral y educativo, salvo supuestos médicos o de seguridad expresamente definidos por ley y compatibles con las garantías constitucionales. Ninguna autoridad podrá condicionar el acceso a una prestación, servicio o trámite público a la inscripción biométrica si no existe habilitación legal expresa, necesidad estricta y una alternativa no biométrica equivalente, accesible y no discriminatoria.

14. Las entidades privadas no podrán desplegar sistemas de identificación biométrica remota para realizar vigilancia general de la población ni operar bases policiales propias. La comunicación de imágenes o datos a una autoridad

deberá cumplir la legislación especial, responder a una solicitud motivada y quedar sujeta a registro, limitación de finalidad y prohibición de reutilización.

Artículo 101. Videovigilancia en comunidades residenciales. Las juntas de condominio, asociaciones de vecinos y demás formas de gestión de comunidades residenciales podrán instalar sistemas de videovigilancia en las zonas comunes con fines de seguridad, siempre que: 1. La instalación haya sido aprobada por la asamblea de propietarios. 2. La ubicación de las cámaras respete la intimidad de las viviendas. 3. Se informe a los residentes. 4. Se designe a una persona natural o jurídica como responsable del tratamiento.

La aprobación de la instalación de cámaras por la asamblea de propietarios no constituirá habilitación suficiente para captar, identificar, autenticar o elaborar perfiles biométricos de residentes, trabajadores, visitantes o terceros. Cualquier tratamiento biométrico deberá cumplir los artículos 17, 24, 25 y 25 bis y contar con habilitación y finalidad específicas.

Artículo 102. Videovigilancia en centros educativos. Los centros educativos podrán instalar sistemas de videovigilancia en zonas comunes y perimetrales, con fines de seguridad y protección de la comunidad educativa, siempre que: 1. La instalación esté justificada en un plan de seguridad institucional. 2. Se respete el interés superior de niños, niñas y adolescentes. 3. Se informe a la comunidad educativa. 4. Quede prohibida la videovigilancia en aulas de clase durante el desarrollo de actividades pedagógicas.

La autorización para instalar videovigilancia en zonas comunes o perimetrales no habilitará el reconocimiento facial o biométrico generalizado de estudiantes, docentes, trabajadores o visitantes. Queda prohibido utilizar biometría para controlar de manera generalizada la asistencia, el comportamiento o los desplazamientos de niños, niñas y adolescentes, salvo habilitación expresa mediante norma con rango de ley para una finalidad específica de protección, con estricta necesidad, proporcionalidad, evaluación de impacto y garantías reforzadas del interés superior del niño.

Artículo 103. Acceso de autoridades a sistemas privados de videovigilancia. Los cuerpos de seguridad pública podrán instalar y operar sistemas de videovigilancia en espacios públicos en ejercicio de competencias constitucionales y legales, con sujeción a los artículos 17, 24, 25, 47, 100 y 128 de esta Ley y a la legislación especial. El acceso a grabaciones o imágenes procedentes de sistemas privados requerirá orden judicial motivada o una habilitación legal expresa para una investigación o situación concreta, con delimitación de finalidad, período, personas autorizadas, datos solicitados, plazo de conservación y trazabilidad. La sola propiedad, posesión o administración de una cámara no convierte al titular del inmueble en representante de todas las personas captadas ni sustituye la base jurídica para comunicar sus datos. La entrega voluntaria solo será admisible cuando concurra una base legal propia, sea necesaria para evitar un riesgo inminente o atender una obligación legal y se limite a lo estrictamente indispensable. La comunicación a inteligencia se someterá a las restricciones del artículo 50 y a la ley especial aplicable.

El acceso, obtención, comunicación y utilización por cuerpos de seguridad pública de imágenes captadas por sistemas privados requerirá competencia legal de la autoridad solicitante y habilitación para la finalidad concreta. La solicitud será motivada, específica y limitada a período, lugar, categorías de personas y datos estrictamente necesarios. Cuando la ley exija autorización judicial, esta será obligatoria. La titularidad del sistema o la autorización de su propietario no sustituirán la habilitación legal para tratar los datos de las personas grabadas. Toda comunicación quedará registrada y será auditable.

Artículo 104. Cláusula de especialidad y remisión. Las disposiciones de este Título se aplicarán supletoriamente al régimen de videovigilancia laboral establecido en el Título X de esta Ley. En caso de conflicto interpretativo, prevalecerá la norma más protectora de los derechos del interesado.

TÍTULO XII

DERECHOS DIGITALES DEL CIUDADANO

Artículo 105. Ámbito y anclaje constitucional. Este Título desarrolla derechos fundamentales del ciudadano en el entorno digital, en interpretación de los artículos 21, 23, 26, 28, 48, 49, 57, 58, 60, 108 y 143 de la Constitución, con especial atención a la libertad de expresión e información, privacidad, comunicaciones, acceso a registros y tutela judicial.

Artículo 106. Derecho a la neutralidad de Internet. Toda persona tiene derecho a acceder a Internet sin discriminación arbitraria por parte de los prestadores de conexión respecto de contenidos, aplicaciones o servicios

lícitos. Los prestadores no podrán bloquear, degradar o filtrar contenidos salvo por razones técnicas objetivas, necesarias y transparentes de gestión de tráfico o seguridad de la red, o en cumplimiento de orden judicial específica, motivada, proporcional, temporal y susceptible de revisión. Ninguna disposición de este artículo habilita bloqueos generales, censura previa ni restricciones administrativas indeterminadas.

Artículo 107. Derecho de acceso universal a Internet. El Estado promoverá el acceso universal a Internet como derecho instrumental para el ejercicio de los derechos fundamentales en el entorno digital. A tal efecto, adoptará políticas públicas orientadas a: 1. Ampliar la cobertura territorial de las redes de telecomunicaciones. 2. Promover la asequibilidad económica de los servicios de conexión. 3. Garantizar el acceso a Internet en centros educativos, bibliotecas, centros de salud y espacios comunitarios. 4. Facilitar la conectividad de personas con discapacidad mediante tecnologías adaptadas.

Artículo 108. Derecho a la seguridad digital. Todo ciudadano tiene derecho a que los prestadores de servicios digitales adopten medidas técnicas y organizativas apropiadas para garantizar la seguridad de sus datos personales y de sus comunicaciones en el entorno digital.

Artículo 109. Derecho a la educación digital. Todo ciudadano tiene derecho a recibir educación digital como componente del derecho fundamental a la educación consagrado en la Constitución. La educación digital comprende: alfabetización digital básica; conocimiento de los derechos que asisten al ciudadano en el entorno digital; formación en pensamiento crítico frente a la desinformación y la manipulación algorítmica; y formación específica para el uso ético y responsable de la inteligencia artificial.

Artículo 110. Derecho al olvido en motores de búsqueda. El interesado podrá solicitar la desindexación de resultados que asocien su nombre con información inexacta, no pertinente, excesiva o desactualizada, cuando carezca de interés público actual y afecte injustificadamente sus derechos. La decisión deberá ponderar, caso por caso, la veracidad, actualidad, contexto, relevancia pública, naturaleza de la información, papel público de la persona, tiempo transcurrido, interés histórico, libertad de expresión e información y derechos de terceros. La desindexación no implica necesariamente la supresión de la fuente original. El responsable comunicará una decisión motivada y ofrecerá vía de reclamación.

Artículo 111. Derecho de supresión en redes sociales y servicios equivalentes. El interesado podrá solicitar la supresión de datos personales publicados por él mismo o por terceros cuando sean ilícitos, inexactos, excesivos, hayan perdido pertinencia o concurra otra causa legal. El prestador ponderará la libertad de expresión e información, el interés público, la investigación periodística, los archivos históricos, la memoria de violaciones de derechos humanos y la protección de víctimas y menores. La ponderación no crea una inmunidad para información falsa o ilícita ni un derecho a borrar automáticamente hechos veraces de interés público; la resolución deberá motivarse y ser revisable.

Artículo 112. Coordinación institucional y desarrollo reglamentario. La aplicación de los derechos reconocidos en este Título requerirá la coordinación entre la Superintendencia Nacional de Protección de Datos Personales y la Comisión Nacional de Telecomunicaciones, el Ministerio del Poder Popular con competencia en materia educativa, el Ministerio del Poder Popular con competencia en materia de ciencia y tecnología, y los cuerpos de seguridad ciudadana.

TÍTULO XIII

TRANSFERENCIAS INTERNACIONALES DE DATOS

Artículo 113. Principio general. La transferencia internacional de datos personales solo será lícita cuando se garantice un nivel de protección equivalente al establecido en esta Ley.

Artículo 114. Países con nivel adecuado de protección. Podrán realizarse transferencias internacionales sin autorización previa a países u organizaciones internacionales reconocidos por la Superintendencia como poseedores de un nivel adecuado de protección. La evaluación atenderá al Estado de Derecho, respeto de derechos humanos, legislación aplicable, independencia y eficacia de la autoridad de control, vías administrativas y judiciales, reglas de acceso por autoridades públicas, limitaciones a transferencias ulteriores y garantías efectivas para los interesados. El reconocimiento será motivado, público, revisable periódicamente y podrá suspenderse o retirarse cuando desaparezcan las condiciones que lo justificaron.

Artículo 115. Cláusulas contractuales tipo. En ausencia de decisión de adecuación, podrá realizarse la transferencia cuando el responsable o encargado aporte garantías adecuadas mediante cláusulas contractuales tipo

aprobadas por la Superintendencia. Las cláusulas deberán regular derechos exigibles, auditoría, seguridad, notificación de brechas, acceso de autoridades públicas, transferencias ulteriores, supresión y mecanismos de reclamación. La Superintendencia aprobará y publicará modelos de cláusulas dentro de los seis meses siguientes a su instalación. Mientras se aprueban, podrán utilizarse garantías contractuales específicas que cumplan las exigencias de esta Ley, queden documentadas en la evaluación de impacto cuando corresponda y sean sometidas a control posterior.

Artículo 116. Normas corporativas vinculantes. Los grupos empresariales podrán establecer normas corporativas vinculantes para regir las transferencias intragrupo de datos personales. Las normas deberán ser aprobadas por la Superintendencia.

Artículo 117. Excepciones tasadas y urgencia. En ausencia de decisión de adecuación y de garantías adecuadas, la transferencia solo podrá realizarse excepcionalmente cuando concurra uno de los siguientes supuestos: consentimiento explícito, específico e informado para una transferencia concreta; necesidad estricta para un contrato solicitado por el interesado; interés público esencial reconocido en una norma con rango de ley; formulación, ejercicio o defensa de reclamaciones; protección de intereses vitales; o una transferencia ocasional, no repetitiva y limitada que no pueda realizarse razonablemente mediante otro mecanismo y respecto de la cual el responsable documente necesidad, proporcionalidad y garantías. En situaciones urgentes de riesgo real e inmediato para la vida o integridad, la transferencia mínima indispensable podrá efectuarse para proteger intereses vitales, con registro, comunicación posterior a la Superintendencia cuando sea posible y revisión ex post. La urgencia no habilita transferencias masivas, estructurales, recurrentes ni el acceso general de autoridades extranjeras; tampoco permite eludir tratados vigentes, derechos constitucionales o las garantías de los artículos 113 a 116.

Artículo 118. Autorización de la Superintendencia. Fuera de los supuestos anteriores, la transferencia internacional requerirá autorización previa de la Superintendencia.

TÍTULO XIV

SUPERINTENDENCIA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

Capítulo I. Naturaleza, adscripción e independencia

Artículo 119. Creación, naturaleza jurídica e independencia. Se crea la Superintendencia Nacional de Protección de Datos Personales como ente público especializado de derecho, con personalidad jurídica y patrimonio propios y autonomía funcional, técnica, administrativa, financiera y de personal, configurado como autoridad administrativa independiente para el ejercicio de sus competencias de supervisión y garantía. No estará sometida a instrucciones jerárquicas de sujetos regulados ni a tutela de órganos que puedan revisar o condicionar decisiones concretas de inspección, reclamación o sanción. La Superintendencia no constituye un Poder Público adicional ni se sitúa fuera del orden constitucional. Su adscripción o vinculación administrativa instrumental, exclusivamente para coordinación general, soporte presupuestario y gestión administrativa no decisoria, deberá definirse por ley de modo compatible con los artículos 136, 140, 141, 142 y 273 a 274 de la Constitución, sin dependencia funcional ni instrucciones sobre casos. Se recomienda, como opción de mayor prudencia constitucional, una entidad pública autónoma de supervisión con independencia funcional reforzada, sometida al sistema nacional de control fiscal, control jurisdiccional y rendición de cuentas institucional, sin integrarla artificialmente como órgano de la Contraloría, Fiscalía o Defensoría ni crear una sexta rama.

Artículo 120. Autonomía y garantías institucionales. La autonomía comprende: 1. Independencia funcional para ejercer sus competencias sin instrucciones sobre casos concretos. 2. Autonomía financiera y presupuestaria dentro del sistema presupuestario y de control fiscal de la República. La Superintendencia formulará su anteproyecto presupuestario y lo remitirá directamente a la Asamblea Nacional y a los órganos presupuestarios competentes; su asignación se identificará de forma diferenciada, sin excluir los controles constitucionales. 3. Autonomía administrativa y de organización interna, conforme a la ley. 4. Autonomía de personal, con ingreso por mérito, estabilidad e incompatibilidades legales. 5. Control fiscal interno y externo por los órganos constitucionalmente competentes, sin interferencia en expedientes ni decisiones técnicas. 6. Rendición anual pública de cuentas ante la Asamblea Nacional, publicación de memoria de gestión, estadísticas, presupuesto ejecutado, auditorías y criterios generales, con reserva de datos personales y expedientes. Ninguna autoridad podrá condicionar recursos o personal para influir en una actuación concreta.

Artículo 121. Independencia funcional. En el ejercicio de sus funciones de supervisión, garantía, investigación y sanción, la Superintendencia y su personal actuarán con independencia y sin instrucciones sobre expedientes concretos. La independencia se ejercerá con transparencia, motivación, responsabilidad, publicidad de criterios generales y control jurisdiccional posterior. Todo conflicto de interés deberá declararse y dar lugar a inhibición. Se

prohíben interferencias indebidas de órganos públicos, sujetos regulados o terceros, sin perjuicio de los mecanismos constitucionales de control fiscal, rendición de cuentas y responsabilidad.

Capítulo II. Órganos superiores de dirección

Artículo 122. Órganos superiores. La Superintendencia estará compuesta por los siguientes órganos superiores: 1. El Superintendente Nacional, órgano unipersonal de dirección y representación institucional. 2. Dos Superintendentes Adjuntos, con funciones de asistencia directa, coordinación de áreas estratégicas y suplencia institucional. 3. El Consejo Consultivo, órgano colegiado de asesoramiento normativo, deliberación estratégica y emisión de criterios interpretativos. La dirección técnica del organismo se ejercerá de manera colegiada entre el Superintendente Nacional y los Superintendentes Adjuntos, en los términos previstos por el reglamento interno.

Artículo 123. Superintendente Nacional. El Superintendente Nacional ejerce la representación institucional. Le corresponde: 1. Presidir la Superintendencia y coordinar a los Adjuntos. 2. Dictar las resoluciones finales de los procedimientos sancionadores con separación respecto de la fase instructora. 3. Aprobar criterios técnicos generales en el marco de la Ley. 4. Representar a la Superintendencia ante órganos públicos y autoridades extranjeras. 5. Suscribir acuerdos de cooperación. 6. Convocar y presidir el Consejo Consultivo. 7. Aprobar el anteproyecto de presupuesto y el informe de gestión para su remisión directa a la Asamblea Nacional y a los órganos de control fiscal competentes. 8. Las demás competencias atribuidas expresamente por esta Ley.

Artículo 124. Superintendentes Adjuntos. La Superintendencia contará con dos Superintendentes Adjuntos, con rango equivalente al de Dirección General, encargados de coordinar las áreas estratégicas del organismo. Les corresponde: 1. Asistir directamente al Superintendente Nacional en el ejercicio de sus funciones. 2. Coordinar las Subdirecciones especializadas cuya supervisión les sea asignada por el Superintendente Nacional mediante resolución motivada. 3. Suplir al Superintendente Nacional en los supuestos de ausencia temporal, vacancia o inhibición, conforme al orden que determine el reglamento interno. 4. Adoptar, por delegación expresa del Superintendente Nacional, resoluciones en procedimientos administrativos no sancionadores. 5. Las demás competencias que les atribuyan esta Ley y el reglamento interno.

Artículo 125. Consejo Consultivo. Composición. El Consejo Consultivo estará integrado por representantes con experiencia acreditada en protección de datos, derechos humanos, tecnología y sectores regulados: 1. Un representante designado por la Asamblea Nacional. 2. Dos representantes del sector universitario, uno de Derecho y otro de informática o ciencia de datos, seleccionados mediante convocatoria pública. 3. Un representante de colegios profesionales jurídicos. 4. Un representante de organizaciones de derechos humanos o derechos digitales. 5. Un representante de organizaciones de consumidores o usuarios. 6. Un representante de trabajadores y sus organizaciones. 7. Un representante de sectores productivos y tecnológicos. Los órganos de investigación penal, seguridad e inteligencia podrán participar como invitados técnicos, sin voto cuando exista conflicto de interés o se debatan expedientes que les afecten. Los miembros tendrán períodos fijos, causales tasadas de remoción, declaración de intereses y deber de abstención. La remoción no dependerá exclusivamente de la voluntad discrecional de la institución designante.

Artículo 126. Consejo Consultivo. Funciones. Corresponden al Consejo Consultivo las siguientes funciones: 1. Emitir dictamen preceptivo, no vinculante, sobre los proyectos de reglamento y de instrucciones generales que la Superintendencia se proponga aprobar. 2. Emitir dictamen preceptivo, no vinculante, sobre las decisiones de la Superintendencia relativas al reconocimiento del nivel adecuado de protección de países terceros y a la aprobación de códigos de conducta sectoriales de alcance general. 3. Formular propuestas al Superintendente Nacional sobre las orientaciones estratégicas del organismo. 4. Emitir informes de propia iniciativa sobre cuestiones normativas o interpretativas de alcance general. 5. Servir de canal institucional de deliberación entre la Superintendencia y los sectores representados. El Consejo Consultivo se reunirá al menos trimestralmente, y sus deliberaciones y dictámenes serán objeto de publicidad en el portal oficial de la Superintendencia, salvo cuando la naturaleza reservada de la materia lo desaconseje.

Capítulo III. Estructura operativa

Artículo 127. Estructura operativa. Bajo la dirección superior del Superintendente Nacional y de los Superintendentes Adjuntos, la Superintendencia se organiza en las siguientes unidades operativas: 1. Secretaría General, encargada de la gestión de recursos humanos, régimen económico-financiero, presupuestario, contratación pública, registros administrativos generales y coordinación operativa interna. 2. Subdirección General de Inspección de Datos, encargada de la tramitación de reclamaciones, investigación de oficio de brechas de seguridad,

inspecciones en sede del responsable o del encargado, fase instructora de los procedimientos sancionadores y propuesta de medidas correctoras. 3. Subdirección General de Promoción y Autorizaciones, encargada de la divulgación normativa, fomento de códigos de conducta, gestión del Registro Nacional de Tratamientos, gestión del Registro de Delegados de Protección de Datos, atención ciudadana, y tramitación de autorizaciones relativas a transferencias internacionales y demás autorizaciones previstas en esta Ley. 4. Servicios Jurídicos, encargados del asesoramiento legal interno, representación en juicio, relaciones internacionales y participación en foros y redes internacionales de autoridades de control. Reglamentariamente se determinará la estructura interna de cada unidad, la asignación específica de funciones y los mecanismos de coordinación entre ellas.

Artículo 128. Coordinación institucional, inventario de sistemas y límites de acceso. La Superintendencia podrá establecer protocolos de coordinación con el Ministerio Público, cuerpos de seguridad ciudadana, órganos de inteligencia, autoridades electorales, registros, banca, telecomunicaciones, educación y demás autoridades concurrentes. La coordinación no confiere acceso genérico, permanente ni indiscriminado a bases personales, biométricas, electorales o de víctimas, ni sustituye las competencias constitucionales del CNE, autoridades de identidad, registros civiles, órganos de seguridad o jurisdicción. Todo intercambio deberá contar con base legal específica, finalidad determinada, necesidad y proporcionalidad, identificación del emisor y receptor, funcionarios autorizados, categorías mínimas de datos, plazo de conservación, prohibición de reutilización y registro auditable. Los órganos de inteligencia solo accederán cuando exista habilitación legal expresa y control judicial o independiente conforme a ley especial. La Superintendencia, en coordinación —no subordinación ni sustitución— con cada autoridad competente, elaborará y mantendrá un inventario jurídico-técnico de sistemas estatales de tratamiento de datos, que identificará para cada sistema: órgano responsable y encargado; ley habilitante y Gaceta Oficial; finalidad; fuente y categorías de datos; interoperabilidad y destinatarios; base de legitimación; conservación; transferencias; medidas de seguridad; evaluación de impacto; auditoría y régimen de control. El inventario tendrá versión pública con información no sensible y anexos reservados sujetos a control legal. CNE, SAIME, registros y demás autoridades conservarán sus competencias constitucionales y sectoriales.

Capítulo IV. Nombramiento, período y remoción

Artículo 129. Nombramiento y proceso de selección. El Superintendente Nacional y los Superintendentes Adjuntos serán designados por la Asamblea Nacional con el voto favorable de las dos terceras partes de sus integrantes. La selección partirá de un procedimiento público, abierto y basado en méritos, integridad, experiencia y conocimiento interdisciplinario, convocado por una comisión plural de evaluación creada por esta Ley, con participación transparente de universidades, colegios profesionales y organizaciones de la sociedad civil. Se publicarán requisitos, postulaciones, declaraciones de intereses, criterios de evaluación y puntuaciones motivadas, y se garantizarán observaciones ciudadanas y entrevistas públicas. La comisión propondrá una lista de candidaturas elegibles; la Asamblea realizará la designación conforme a la Constitución. El artículo 279 constitucional se toma como referencia de participación pública, sin extender automáticamente su ámbito a esta autoridad.

Artículo 130. Períodos escalonados. El período del Superintendente Nacional y de los Superintendentes Adjuntos será de siete años. Los períodos serán escalonados de modo que no coincidan entre sí ni con el ciclo electoral del Poder Ejecutivo. Podrán ser reelegidos por una sola vez, mediante el mismo procedimiento previsto para su designación. La transición entre períodos garantizará la continuidad del funcionamiento institucional.

Artículo 131. Requisitos e incompatibilidades. Para ser Superintendente Nacional o Adjunto se requiere: ser venezolano por nacimiento o naturalización, mayor de treinta y cinco años, con al menos diez años de ejercicio profesional en áreas relacionadas con el derecho, la tecnología, la ciencia de datos o disciplinas afines. Son incompatibilidades con el ejercicio del cargo: la afiliación a partidos políticos; el ejercicio profesional privado remunerado; el desempeño de cargos directivos en organizaciones responsables o encargadas de tratamientos sujetos al control de la Superintendencia; y cualquier otra que reglamentariamente se determine para preservar la independencia. Las incompatibilidades se extenderán durante los dos años siguientes al cese en el cargo.

Artículo 132. Causales y procedimiento de remoción. El Superintendente Nacional y los Superintendentes Adjuntos solo podrán ser removidos por causas taxativas establecidas en esta Ley: incapacidad permanente debidamente acreditada; condena penal firme por delito doloso incompatible con el cargo; incumplimiento grave y culpable de deberes esenciales; conflicto de interés grave no subsanado; o renuncia. La remoción por falta grave requerirá procedimiento contradictorio, notificación, acceso al expediente, defensa, prueba, decisión motivada de la Asamblea Nacional por mayoría de dos tercios y posibilidad de control jurisdiccional. Ningún órgano que sea sujeto regulado podrá calificar por sí solo la falta grave ni vetar la remoción.

Capítulo V. Competencias y procedimiento sancionador

Artículo 133. Competencias. Son competencias de la Superintendencia: 1. Velar por el cumplimiento de esta Ley. 2. Administrar el Registro Nacional de Tratamientos. 3. Recibir y tramitar reclamaciones. 4. Investigar de oficio y tramitar procedimientos sancionadores. 5. Ordenar la cesación de tratamientos ilícitos y medidas cautelares conforme a la Ley. 6. Aprobar códigos de conducta y cláusulas tipo dentro de los límites legales. 7. Autorizar transferencias cuando la Ley lo requiera. 8. Ordenar auditorías y evaluaciones de impacto en los supuestos previstos. 9. Emitir informes públicos y recomendaciones. 10. Cooperar con autoridades de control extranjeras conforme a tratados y garantías. 11. Publicar guías, criterios y estudios técnicos no vinculantes salvo habilitación legal expresa. 12. Coordinar conforme al artículo 128. 13. Aprobar su organización interna y anteproyecto de presupuesto. 14. Dictar normas técnicas de ejecución estrictamente subordinadas a esta Ley, sin crear bases de legitimación, excepciones materiales, infracciones, sanciones, competencias, sujetos obligados o finalidades biométricas nuevas.

Artículo 134. Procedimiento administrativo sancionador y prescripción. El procedimiento sancionador se iniciará de oficio o por denuncia y garantizará legalidad, tipicidad, culpabilidad, presunción de inocencia, audiencia, defensa, contradicción, prueba, motivación, proporcionalidad y non bis in idem. La fase instructora estará separada orgánica y funcionalmente de la autoridad que resuelva. La carga de acreditar la infracción corresponderá a la Administración. El procedimiento tendrá una duración máxima de doce meses, prorrogable una sola vez por hasta seis meses mediante decisión motivada notificada antes del vencimiento. Vencido el plazo sin resolución se producirá la caducidad del procedimiento, sin perjuicio de iniciar otro mientras la infracción no haya prescrito y no exista cosa decidida o vulneración del non bis in idem. Para consulta se propone prescripción de las infracciones leves a los dos años, graves a los tres y muy graves a los cinco. El cómputo comenzará el día siguiente a la comisión; en infracciones permanentes o continuadas, desde que cese la conducta o se realice el último acto que la integra. La prescripción se suspenderá únicamente desde la notificación formal de la imputación y durante la tramitación válida del procedimiento, sin exceder su plazo máximo legal; se reanudará por el tiempo restante cuando se declare la caducidad o finalice el procedimiento sin sanción firme. Las actuaciones preliminares no notificadas no suspenderán ni interrumpirán el cómputo. Las sanciones prescribirán en iguales plazos desde el día siguiente a la firmeza de la resolución; el cómputo solo podrá suspenderse por una decisión judicial que impida su ejecución, durante el tiempo en que dicha decisión esté vigente. El silencio negativo de peticiones o recursos administrativos se regirá separadamente por la legislación administrativa y no se confundirá con la caducidad del procedimiento sancionador. Estos plazos constituyen una propuesta legislativa que deberá ser evaluada en consulta y justificada en la Exposición de Motivos.

Artículo 135. Tipificación cerrada de infracciones. Las infracciones a esta Ley son exclusivamente las tipificadas en este artículo; ninguna infracción, elemento esencial, agravante, categoría sancionable o sanción podrá crearse, ampliarse o agravarse por reglamento, resolución o criterio administrativo. Son infracciones leves: a) incumplir deberes formales de información sin afectar materialmente los derechos; b) atender fuera de plazo una solicitud de derechos sin causa justificada, cuando no concurra reiteración ni daño relevante; c) mantener errores formales en el registro interno que se corrijan oportunamente. Son infracciones graves: a) tratar datos sin base de legitimación; b) incumplir deberes de información, acceso, rectificación, supresión u oposición de forma sustancial; c) omitir una evaluación de impacto legalmente obligatoria; d) no designar delegado cuando sea exigible; e) incumplir medidas de seguridad o contratos de encargado sin riesgo grave a la vida o integridad; f) realizar transferencia internacional sin garantías exigibles; g) incumplir reglas de videovigilancia o geolocalización; h) no notificar una brecha dentro del plazo legal, cuando no exista riesgo vital; i) incumplir una orden individual, motivada y legalmente ejecutiva de la Superintendencia, válidamente notificada, una vez vencido el plazo concedido para su cumplimiento. Son infracciones muy graves: a) tratar categorías especiales o ultrasensibles sin habilitación legal; b) desplegar sistemas biométricos prohibidos o sin la base y excepción exigidas; c) crear o ampliar bases de reconocimiento facial mediante extracción indiscriminada; d) realizar identificación biométrica remota masiva o exploratoria contraria al artículo 100; e) acceder, comunicar, ceder o reutilizar datos biométricos sin competencia o habilitación; f) conservar plantillas tras extinguirse la finalidad o habilitación legal sin causa válida; g) manipular deliberadamente parámetros para provocar falsos positivos o encubrir sesgos; h) ocultar, destruir o alterar registros de acceso o auditoría; i) incumplir el deber agravado de notificación de una brecha con riesgo para la vida o integridad; j) adoptar medidas de seguridad manifiestamente insuficientes que generen un riesgo grave y acreditado para la vida o integridad; k) tomar represalias contra denunciantes, titulares o quienes ejerzan derechos; l) utilizar datos para persecución política, discriminación o represalia; m) reincidir específicamente en una infracción grave, mediante nueva conducta sustancialmente equivalente dentro de los tres años siguientes a la firmeza de una sanción anterior por esa conducta. La responsabilidad exigirá dolo o culpa, y la sanción se graduará conforme al artículo 137.

Artículo 136. Sanciones y criterios de cuantificación. Las sanciones podrán consistir en amonestación, multa, orden de adecuación, limitación o cesación del tratamiento y, en los casos más graves, inhabilitación temporal para una operación o

categoría de tratamiento. Queda excluida la inhabilitación definitiva. Para personas jurídicas, el límite máximo de multa podrá alcanzar hasta el dos por ciento del volumen de negocios anual global en infracciones graves y hasta el cuatro por ciento en infracciones muy graves, aplicándose el límite que resulte legalmente válido y proporcional. La base de cálculo será el volumen de negocios del ejercicio económico inmediatamente anterior, debidamente acreditado, y deberán definirse reglas especiales para entidades de reciente creación, grupos empresariales y ausencia de ingresos. Para personas naturales, entidades sin fines de lucro y entes públicos deberán establecerse escalas diferenciadas, con cuantías mínimas y máximas expresadas en bolívares, criterios de capacidad económica, gravedad, beneficio obtenido y daño causado. La cuantía monetaria de cada escala deberá quedar fijada de manera taxativa en el texto legal antes de su consignación; mientras no se establezca, no podrá imponerse multa a esos sujetos por analogía ni mediante remisión al reglamento. No se utilizará la unidad tributaria sin verificación oficial de su vigencia y régimen aplicable. La inhabilitación temporal no excederá de cinco años, deberá motivarse y será revisable en los términos de la Ley.

Artículo 137. Criterios de graduación. La determinación de la sanción tendrá en cuenta: la naturaleza, gravedad y duración de la infracción; el número de interesados afectados y el nivel de daño; la intencionalidad o negligencia; las medidas técnicas y organizativas aplicadas; las infracciones anteriores; el grado de cooperación con la Superintendencia; las categorías de datos afectadas; la forma en que la Superintendencia tuvo conocimiento; y la adopción voluntaria de códigos de conducta o certificaciones. Se aplicará también el principio de proporcionalidad respecto a la capacidad económica del infractor.

Artículo 138. Recursos y tutela judicial. Contra las resoluciones sancionatorias podrá interponerse recurso potestativo de reconsideración ante la Superintendencia dentro de los quince (15) días hábiles siguientes a su notificación, conforme a la regla de cómputo prevista en el artículo 42 de la Ley Orgánica de Procedimientos Administrativos. La Superintendencia deberá resolverlo mediante decisión motivada dentro de los treinta (30) días hábiles siguientes a su presentación. El vencimiento de ese plazo sin decisión producirá únicamente el efecto de habilitar el acceso a la jurisdicción contencioso-administrativa y no se confundirá con la caducidad del procedimiento sancionador. El recurso de reconsideración no será requisito obligatorio para acudir a la jurisdicción; cuando se interponga, el plazo judicial se computará desde la notificación de la decisión o desde el vencimiento del plazo legal para resolver, conforme a la Ley Orgánica de la Jurisdicción Contencioso Administrativa. La interposición del recurso no suspenderá automáticamente la ejecución, pero la Superintendencia o el tribunal competente podrán acordar medidas cautelares cuando la ejecución pueda causar perjuicio grave o de difícil reparación, o cuando se alegue y resulte plausible la nulidad absoluta del acto. La notificación de la resolución indicará de forma precisa los recursos procedentes, autoridad competente, forma de interposición y lapsos aplicables. Ninguna disposición restringe el derecho de acceso a la justicia ni el control judicial de los actos de la Superintendencia.

Artículo 139. Cooperación internacional. La Superintendencia cooperará con autoridades de control de otros países y organismos internacionales especializados en el marco de tratados vigentes y acuerdos celebrados dentro de sus competencias. Todo intercambio de datos personales deberá contar con base legal, finalidad específica, necesidad, proporcionalidad, confidencialidad, seguridad, registro de accesos, límites de conservación y prohibición de utilización ulterior incompatible. No se comunicarán datos de víctimas, testigos, personas protegidas o categorías especiales salvo habilitación legal suficiente y garantías concretas. La cooperación no podrá utilizarse para eludir las garantías constitucionales ni para dar acceso genérico a bases de datos nacionales.

MATRIZ DE COMPATIBILIDAD TEMPORAL (GUÍA DE CONSULTA). Antes de la consignación se comprobará en una tabla única la secuencia: entrada en vigor; instalación de la Superintendencia (máximo nueve meses); inventario inicial biométrico y estatal (seis meses desde instalación); especificaciones del Registro (seis meses desde instalación) y registro operativo (doce meses desde aprobación); adecuación general (dieciocho meses desde instalación); adecuación de videovigilancia (dieciocho meses desde instalación); adecuación biométrica legalmente habilitada (hasta doce meses desde aprobación del plan); cese/sustitución de biometría laboral no habilitada (seis meses desde entrada en vigor); reglamentos y auditorías. La tabla deberá identificar responsable, fecha inicial, fecha final, dependencia, consecuencia del incumplimiento y derechos que no pueden quedar suspendidos. Los plazos reglamentarios no podrán prorrogar prohibiciones ni postergar garantías directamente exigibles.

DISPOSICIONES TRANSITORIAS

Disposición Transitoria Primera. Instalación y puesta en funcionamiento. La Superintendencia se instalará dentro de los nueve meses siguientes a la entrada en vigor de esta Ley, mediante el procedimiento de selección y designación previsto en los artículos 129 a 132. Dentro de los primeros noventa días se constituirá la comisión de evaluación y se publicará el calendario de convocatoria, selección y designación. En caso de actuaciones preparatorias, la Asamblea Nacional podrá

designar por mayoría de dos tercios una Comisión Instaladora temporal, exclusivamente presupuestaria, administrativa y organizativa, sin potestad de inspección, reclamación ni sanción. La Defensoría del Pueblo conservará las competencias y legitimaciones constitucionales; no asumirá provisionalmente potestades regulatorias o sancionadoras no atribuidas por la Constitución.

Disposición Transitoria Segunda. Plazo general de adecuación. Los responsables y encargados dispondrán de dieciocho meses contados desde la instalación efectiva de la Superintendencia para adecuar los tratamientos preexistentes que puedan continuar legalmente. Este plazo no ampara prácticas prohibidas desde la entrada en vigor, tratamientos carentes de base jurídica, ni incumplimientos que comprometan de forma grave la vida, la integridad o derechos fundamentales. La ausencia de la Superintendencia no suspende los derechos de los titulares ni la tutela judicial.

Disposición Transitoria Tercera. Registro Nacional de Tratamientos y hitos técnicos. La Superintendencia aprobará dentro de los seis meses siguientes a su instalación las especificaciones y fases del Registro Nacional de Tratamientos y publicará modelos de cláusulas contractuales tipo para transferencias internacionales conforme al artículo 115. El registro inicial estará operativo dentro de los doce meses siguientes a la aprobación de especificaciones. Se priorizarán organismos públicos, tratamientos de alto riesgo y categorías especiales a gran escala. Las auditorías, formularios, reglamentos y especificaciones serán instrumentos de ejecución: no podrán crear obligaciones esenciales, excepciones, infracciones, sanciones ni condicionar el ejercicio de derechos reconocidos directamente por esta Ley.

Disposición Transitoria Cuarta. Delegado de protección de datos. Las entidades obligadas a designar delegado de protección de datos conforme al artículo 48 procederán a su designación dentro del plazo general de adecuación. Reglamentariamente se establecerán los requisitos y el régimen de acreditación de la figura.

Disposición Transitoria Quinta. Coordinación con la CNVJRS. La coordinación con la Comisión Nacional de la Verdad, Justicia, Reparación y Sanación en materia de datos de víctimas, testigos y personas comparecientes se desarrollará conforme a la Constitución, a esta Ley y a la Ley Orgánica de la CNVJRS, si esta última resultare aprobada y vigente. Antes de aprobar el protocolo se verificará la concordancia de ambas leyes, el reparto de competencias, la custodia y acceso a archivos, la protección de identidades, los plazos de conservación y el destino de los expedientes al extinguirse la Comisión. Ningún protocolo podrá ampliar accesos, finalidades o comunicaciones no habilitadas por ley.

Disposición Transitoria Sexta. Testamento digital y régimen post mortem. La Superintendencia dictará, dentro de los dieciocho meses siguientes a su instalación, el reglamento sobre formalización, registro y ejecución del testamento digital, en coordinación con el Servicio Autónomo de Registros y Notarías y demás órganos competentes.

Disposición Transitoria Séptima. Priorización de la legislación complementaria de ciberseguridad. La Asamblea Nacional podrá priorizar, dentro de su agenda legislativa y en ejercicio de sus competencias constitucionales, el estudio de una Ley Orgánica de Ciberseguridad complementaria. La Superintendencia presentará un informe técnico de necesidades y propuestas de coordinación dentro de los doce meses siguientes a su instalación y, posteriormente, informes semestrales mientras se tramite la iniciativa. Esta disposición no predetermina el sentido de la deliberación parlamentaria ni impone al legislador futuro un resultado normativo. Hasta que se apruebe una ley especial, las obligaciones de seguridad del tratamiento se regirán por esta Ley y por las normas sectoriales vigentes.

Disposición Transitoria Octava. Sistemas de videovigilancia preexistentes. Los responsables de sistemas de videovigilancia instalados con anterioridad a la entrada en vigor de esta Ley dispondrán de dieciocho meses, contados desde la instalación de la Superintendencia, para adecuar dichos sistemas a las disposiciones del Título XI, incluyendo la señalización visible, los plazos de conservación y las prohibiciones aplicables.

Disposición Transitoria Novena. Procesos judiciales en curso. Los procesos judiciales de habeas data en curso al momento de la entrada en vigor de esta Ley continuarán tramitándose conforme a las normas vigentes al momento de su inicio, salvo que las partes soliciten expresamente su tramitación conforme al procedimiento previsto en el Título VII.

Disposición Transitoria Décima. Inventario, suspensión y adecuación de tratamientos biométricos preexistentes y sistemas públicos. Dentro de los seis meses siguientes a la instalación de la Superintendencia, los responsables públicos y privados declararán los sistemas de identificación y autenticación biométrica que mantengan, indicando finalidad, base legal, excepción invocada, personas afectadas, proveedores, destinatarios, interoperabilidad, conservación y evaluación de impacto. Las autoridades públicas incorporarán al inventario del artículo 128 la ficha jurídica y técnica de sus sistemas de

identidad, pasaporte, registro civil, electoral, migratorio, consular y de prestación de servicios, sin publicar información reservada. a) Las prácticas prohibidas por esta Ley —incluida la identificación biométrica remota masiva o indiscriminada, la extracción indiscriminada de imágenes para crear bases y los tratamientos sin base legal ni excepción— cesarán desde su entrada en vigor, sin esperar declaración o autorización administrativa. b) Los sistemas preexistentes con habilitación legal específica y que no incurran en prohibición podrán someterse a auditoría independiente, congelación de finalidades, categorías, bases de comparación e interoperabilidades y plan de adecuación no superior a doce meses desde su aprobación. c) Los sistemas biométricos laborales sin habilitación legal expresa deberán cesar o sustituir la función biométrica al vencimiento de un plazo máximo de seis meses desde la entrada en vigor; durante la transición no podrán ampliarse, incorporar nuevas categorías ni producir consecuencias laborales adversas, y deberán ofrecer alternativa no biométrica. d) La preexistencia no genera presunción de licitud ni derecho adquirido a continuar. Se publicará resumen no sensible de finalidad, responsable, base legal, evaluación y plazo; se reservarán solo detalles cuya divulgación comprometa de forma concreta la seguridad. Las decisiones podrán ser objeto de control judicial.

DISPOSICIÓN DEROGATORIA

Disposición Derogatoria Única. Derogaciones y concordancia. La derogación de normas preexistentes se efectuará de manera expresa y específica en el texto que se someta a primera discusión, previa elaboración de una tabla de concordancias que identifique disposición, Gaceta Oficial, vigencia, rango, materia y modificación o derogación propuesta. La cláusula genérica de incompatibilidad no sustituirá este cotejo ni podrá entenderse como derogación tácita de garantías contenidas en otras leyes orgánicas. Mientras se completa la tabla, la aplicación de esta Ley se armonizará con las normas especiales vigentes, conforme a la Constitución, a la jerarquía normativa y al principio de especialidad. La Superintendencia podrá proponer actualizaciones, pero no decidir por sí sola la derogación de normas.

DISPOSICIONES FINALES

Disposición Final Primera. Reglamento general y normas técnicas. El Reglamento general de esta Ley será dictado por el Presidente de la República conforme al artículo 236, numeral 10, de la Constitución, dentro de los dieciocho meses siguientes a la instalación de la Superintendencia y previa consulta pública. El Reglamento no podrá alterar el espíritu, propósito y razón de la Ley, crear nuevas bases de legitimación, excepciones materiales, infracciones, sanciones, competencias, sujetos obligados ni habilitaciones biométricas. La Superintendencia podrá dictar normas técnicas exclusivamente para ejecutar habilitaciones expresas de esta Ley, definir especificaciones y procedimientos internos, y desarrollar garantías técnicas, sin innovar en materias reservadas al legislador.

Disposición Final Segunda. Cláusula interpretativa pro persona. En caso de duda sobre la interpretación de esta Ley o de sus disposiciones reglamentarias, prevalecerá el criterio más favorable al interesado, conforme al principio pro persona.

Disposición Final Tercera. Entrada en vigor y aplicación del régimen sancionador. Esta Ley entrará en vigor a los sesenta días de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela. Las prohibiciones materiales y los derechos de los interesados serán exigibles desde esa fecha, sin perjuicio de los períodos transitorios expresamente previstos para tratamientos que puedan continuar legalmente. La potestad sancionadora administrativa se ejercerá una vez instalada la Superintendencia y aprobadas las normas de procedimiento estrictamente necesarias, sin exceder de doce meses desde la entrada en vigor. La ausencia temporal de la autoridad no legaliza prácticas prohibidas ni impide la tutela judicial, las competencias constitucionales de la Defensoría del Pueblo o las responsabilidades previstas en otras leyes.

Disposición Final Cuarta. Cláusula de revisión. A los cinco años de la entrada en vigor de esta Ley, la Superintendencia elaborará y remitirá a la Asamblea Nacional un informe evaluatorio sobre su aplicación, con propuestas de reforma. En lo sucesivo, el informe se elaborará con periodicidad quinquenal.

ANEXO I. FUENTES NORMATIVAS Y DOCUMENTALES PARA LA CONSULTA

Las fuentes españolas y europeas se citan como referencias comparadas. No atribuyen competencias a autoridades venezolanas ni sustituyen la verificación de las publicaciones oficiales venezolanas. Para la consignación parlamentaria deberán cotejarse las versiones oficiales, reformas y vigencia de cada instrumento.

A. Unión Europea y España

Reglamento (UE) 2016/679 (RGPD), especialmente artículos 3, 4.14, 5, 6, 9, 22, 25, 32 y 35. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Ley Orgánica 3/2018 (LOPDGDD), especialmente artículos 9 y 10; texto consolidado del BOE. URL: https://www.boe.es/eli/es/lo/2018/12/05/3/con

Ley Orgánica 7/2021, de 26 de mayo, sobre tratamientos de datos personales para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y ejecución de sanciones penales; especialmente artículos 4, 7, 8 y 13. URL: https://www.boe.es/eli/es/lo/2021/05/26/7/con

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana; especialmente artículos 8 a 16. URL: https://www.boe.es/eli/es/lo/2015/03/30/4/con

Real Decreto 255/2025, de 1 de abril, por el que se regula el Documento Nacional de Identidad. URL: https://www.boe.es/eli/es/rd/2025/04/01/255

Reglamento (UE) 2025/1208, de 12 de junio de 2025, sobre el refuerzo de la seguridad de los documentos de identidad y de residencia; especialmente artículos 10.3 y 11.6-7 y considerandos 20-23. Consulta: 4 de noviembre de 2026. URL: https://eur-lex.europa.eu/eli/reg/2025/1208/oj

Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial), especialmente artículo 5.1.h y apartados 2-6, y anexo II; versión consolidada consultada a 4 de noviembre de 2026. URL: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:02024R1689-20260727

Agencia Española de Protección de Datos, Guía sobre tratamientos de control de presencia mediante sistemas biométricos, versión noviembre de 2023. En la copia consultada consta la indicación “EN REVISIÓN”; se cita como orientación técnica, no como norma vinculante. URL: https://www.aepd.es/documento/guia-control-presencia-biometrico.pdf

Agencia Española de Protección de Datos, apartado de Biometría y documentos técnicos complementarios. URL: https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia

B. Venezuela: normas y antecedentes que requieren cotejo oficial

Constitución de la República Bolivariana de Venezuela: artículos 21, 23, 26, 28, 48, 49, 57, 58, 60, 78, 89, 108, 136, 142, 143, 203, 236.10, 273, 274, 279, 281, 294 y 336. Verificar texto consolidado y publicación oficial antes de la presentación formal.

Decreto n.º 1.412, de 13 de noviembre de 2014, de reforma de la Ley Orgánica de Identificación, publicado en la Gaceta Oficial extraordinaria n.º 6.155, de 19 de noviembre de 2014. La ficha de la Gaceta puede consultarse en https://www.gacetaoficial.org/2014-11-19-gaceta-oficial-venezuela-6155; la comisión jurídica deberá incorporar el ejemplar oficial íntegro y verificar el texto consolidado vigente.

Providencia Administrativa SAREN n.º 525, de 17 de octubre de 2024, publicada en la Gaceta Oficial n.º 42.987, relativa a medios electrónicos y biométricos en el servicio registral y notarial. Se localizó una copia de la Gaceta alojada en un repositorio jurídico no oficial: https://iusdata.com/wp-content/uploads/2024/10/PROVIDENCIA-ADMINISTRATIVA-525-17OCT24.pdf. Debe cotejarse con el ejemplar oficial de la Gaceta y comprobarse su vigencia, alcance y compatibilidad con la Ley Orgánica General.

Proyecto de Ley Orgánica de Protección de Datos Personales de CENTRAN, V1.3, borrador consolidado para consulta ampliada, Caracas, agosto de 2026. Documento base de la presente consolidación.

C. Advertencias de técnica legislativa y verificación

Las propuestas de reforma y los índices de leyes complementarias deberán pasar por revisión constitucional, penal, procesal, administrativa, laboral, registral, financiera y de técnica legislativa venezolana.

La referencia europea o española no crea por sí sola competencia en Venezuela. Toda potestad pública, excepción biométrica o acceso a bases de datos deberá establecerse en norma venezolana válida y suficientemente precisa.

La Providencia SAREN n.º 525 es una disposición sublegal. La comisión deberá comprobar si su rango resulta suficiente para cada operación de tratamiento y si requiere armonización o modificación tras la entrada en vigor de la Ley General.

Antes de la publicación o consignación formal deberán cotejarse autenticidad, numeración, vigencia, reformas y texto íntegro de todas las normas venezolanas con la Gaceta Oficial y los órganos competentes. La consulta pública no equivale a aprobación legislativa ni a dictamen jurídico definitivo.

D. FUENTES ADICIONALES Y PUNTOS DE COTEJO DE LA V1.5

Constitución de la República Bolivariana de Venezuela: artículos 21, 23, 26, 28, 48, 49, 57, 58, 60, 78, 89, 108, 136, 142, 143, 203, 236.10, 273, 274, 279, 281, 294 y 336. Texto de referencia: https://www.wipo.int/wipolex/es/legislation/details/3981. La versión y Gaceta que se utilicen para el trámite deberán ser cotejadas oficialmente.

Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales: artículos 7 y 8 sobre competencia por materia y actos de altas autoridades. Cotejar texto y reformas en Gaceta Oficial.

Ley Orgánica de Procedimientos Administrativos: artículo 4 sobre silencio administrativo en peticiones y recursos. Distinguir ese efecto de la caducidad de un procedimiento sancionador.

Ley Orgánica para la Protección de Niños, Niñas y Adolescentes: texto de base y reforma parcial publicada en Gaceta Oficial N.º 6.185 Extraordinario de 8 de junio de 2015. Verificar texto consolidado y artículos sobre autonomía, representación, vida privada e imagen.

Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras; Ley del Estatuto de la Función Pública; legislación de seguridad y salud laboral: confirmar textos vigentes, Gacetas y competencias aplicables.

Ley Orgánica de la Defensoría del Pueblo: Gaceta Oficial N.º 37.995 de 5 de agosto de 2004; verificar vigencia y reformas, especialmente las competencias relacionadas con el hábeas data.

Ley de Registro Civil, Ley Orgánica de Identificación, Ley Orgánica de Procesos Electorales, normas del Consejo Nacional Electoral y régimen consular: cotejar textos, vigencia, bases biométricas e interoperabilidad.

Ley sobre Mensajes de Datos y Firmas Electrónicas; Ley de Infogobierno; Ley Orgánica de Telecomunicaciones; Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos; Ley Especial contra los Delitos Informáticos; y normas de registro y notariado: cotejo individual de vigencia y Gaceta.

Reglamento (UE) 2016/679; Reglamento (UE) 2024/1689; Reglamento (UE) 2025/1208; Ley Orgánica española 3/2018; Ley Orgánica española 7/2021; Real Decreto español 255/2025: referencias de derecho comparado, sujetas a comprobación de ámbito y vigencia.

Chile: Ley 21.719. A la fecha de cierre de esta V1.5 (6 de noviembre de 2026), la ley se encontraba publicada con entrada en vigor originalmente prevista para el 1 de diciembre de 2026; la iniciativa de postergar esa vigencia a 1 de diciembre de 2027 seguía en tramitación legislativa. Verificar el resultado final antes de la publicación del proyecto.

Instrumentos internacionales: Pacto Internacional de Derechos Civiles y Políticos (artículo 17) y los instrumentos de derechos humanos vinculantes para Venezuela según su estado de ratificación. Los Principios de la OEA (2021) y los Estándares Iberoamericanos (2017) deben identificarse como parámetros no vinculantes, salvo que otra fuente jurídica les otorgue tal efecto.

Ley Orgánica de Procedimientos Administrativos, Gaceta Oficial N.º 2.818 Extraordinario, de 1 de julio de 1981: artículos 42 (cómputo de términos en días hábiles), 94 (reconsideración) y 105 (recursos contra multas, plazo de decisión). Texto de consulta en WIPO Lex: https://www.wipo.int/wipolex/es/legislation/details/10246. Verificar ejemplar oficial y reformas antes de la consignación.

Gaceta Oficial de la República Bolivariana de Venezuela N.º 43.288, de 5 de enero de 2026: Acuerdo de la Asamblea Nacional que elige a Jorge Rodríguez Gómez como Presidente para el período 2026-2027. Fuente de consulta del sumario: https://www.gacetaoficial.org/2026-01-05-gaceta-oficial-43288. Cotejar el ejemplar íntegro de la Gaceta en el expediente documental.

Advertencia documental: las normas venezolanas identificadas como pendientes de cotejo no deben citarse como vigentes ni utilizarse para fundar una derogación hasta verificar su publicación, reformas y estado jurídico en Gaceta Oficial.

— FIN DEL PROYECTO V1.5 —