ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

LEY DE PROTECCIÓN DE DATOS PERSONALES

ELIECER FEINZAIG MINTZ Y OTROS SEÑORES DIPUTADOS

EXPEDIENTE N° 23.097

DEPARTAMENTO DE SERVICIOS PARLAMENTARIOS
UNIDAD DE PROYECTOS, EXPEDIENTES Y LEYES

NOTA: **A solicitud del proponente, este Departamento no realizó la revisión de errores formales, materiales e idiomáticos que pueda tener este proyecto de ley**

PROYECTO DE LEY

LEY DE PROTECCIÓN DE DATOS PERSONALES

Expediente N° 23.097

ASAMBLEA LEGISLATIVA

En Costa Rica, tradicionalmente se ha entendido que los datos de los ciudadanos forman parte de su derecho a la intimidad, y, por ello, su protección deriva de los artículos 23, 24 y 28 de la Constitución Política.

Este principio ha tenido su desarrollo en la Ley No. 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales (LPDP), la cual se aprobó el 7 de julio de 2011, luego de varios años de trámite en la Asamblea Legislativa. Dicha Ley creó la Agencia de Protección de los Datos Personales de los Habitantes (PRODHAB), órgano encargado de la rectoría en materia de privacidad en Costa Rica.

A casi una década de la aprobación de la LPDP, resulta indispensable una reforma legal integral al marco regulatorio en la materia, por cuatro motivos principales:

Primero: porque la legislación costarricense se inspiró principalmente en la española, en específico en la Ley Orgánica de Protección de Datos Personales No 15/1999 que traspuso la Directiva europea 95/46/CE. Tanto la Ley como la Directiva mencionadas fueron derogadas y sustituidas por el Reglamento General de Protección de Datos Personales (RGPDP) número 2016/679, el cual entró en vigor en la Unión Europea el 25 de mayo de 2018, así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, para el caso de España. El RGPDP, comúnmente conocido como “GDPR” por sus siglas en inglés, es la norma jurídica más avanzada a nivel mundial en materia de protección de datos personales y establece un replanteamiento completo del sistema regulatorio en la materia. Múltiples países en el mundo y en la región, incluidos Panamá, Brasil, y Barbados, han adecuado sus legislaciones internas al estándar marcado por el RGPDP.

Segundo: Costa Rica ha manifestado su intención de adherirse al Convenio 108, el único tratado internacional de alcance global existente hoy en materia de Protección de Datos Personales. Adherirse a este Convenio constituiría el primer paso para que el país gestione una Decisión de Adecuación del Consejo de Europa, que permita al país ser considerado puerto seguro para las transferencias internacionales de datos personales. El país ha iniciado las consultas con dicho Consejo, tendientes a iniciar el trámite de adhesión, lo cual en forma necesaria implicará que la legislación costarricense se adecúe no solo al Convenio, sino también a su Protocolo, que se conoce como “108 +” y sigue precisamente la línea

del RGPDP antes mencionado. Esto nos haría un país atractivo para la inversión digital proveniente de Europa y favorecería igualmente la exportación de servicios digitales desde Costa Rica hacia el masivo mercado europeo.

Tercero: por el proceso de ingreso de Costa Rica a la OCDE, organismo que tiene directrices específicas sobre protección de datos, enfocados sobre todo en la transferencia internacional de datos personales, tan necesaria para la economía digital. En específico, nos referimos a las las: i) *Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales*, de 1980, ii) *Declaración sobre fjujos de datos transfronterizos*, de 1985, y a la *Declaración ministerial sobre la protección de la privacidad de las redes globales*, de 1998. Tales reglas no son del todo compatibles con las disposiciones de nuestra legislación sobre la materia.

Cuarto: porque luego una década de existencia, la legislación actual ha tenido una modesta incidencia en la forma en cómo se tratan los datos personales en Costa Rica en el sector privado, pero en el sector público, la incidencia ha sido prácticamente nula. Si bien no cabría indicar que la legislación ha sido letra muerta, sí se puede asegurar que no ha propiciado un desarrollo suficiente del derecho a la privacidad del habitante. Además, se trata de una legislación desactualizada frente a los retos de la creciente digitalización de la sociedad, y los acontecimientos recientes que se mencionarán más adelante, así lo acreditan.

Los motivos por los cuales la incidencia de la normativa actual ha sido limitada son varios; sin embargo, se señalarán cuatro principales razones:

1. Poca difusión de la normativa entre la ciudadanía, esto no contribuyó a desarrollar un cambio de cultura en materia de privacidad.

2. Una normativa confusa, contradictoria e incompleta que no propició la existencia de un marco legal que ofreciera seguridad jurídica a los ciudadanos, pero sobre todo a las instituciones públicas y privadas, con respecto a las obligaciones materiales que deben cumplir en esta materia.

3. Falta de recursos materiales y humanos para la PRODHAB que le permita asumir el rol protagónico requerido para lograr un estándar adecuado de protección de datos personales, y

4. La falta de regularización del tratamiento de los datos personales por parte del Estado, sus instituciones y empresas.

Sobre este último punto es que el Comité de Políticas de Economía Digital de la OCDE recomendó al Gobierno de Costa Rica elaborar una estrategia de privacidad, que reflejara un enfoque coordinado entre los organismos gubernamentales.

El tratamiento de datos personales en el sector público merece una especial consideración. En los últimos años se han dado casos alarmantes que revelan un

manejo inadecuado e irresponsable de los datos personales de la población. Tres ejemplos recientes así lo revelan:

a) El conocido caso “UPAD”, amén del cual la Presidencia de la República tuvo acceso a datos sensibles de los costarricenses sin Ley que lo autorizara y sin consentimiento de la ciudadanía. Este caso también reveló la ausencia de reglas claras en cuanto a la transferencia de datos entre instituciones, transferencias de las cuales los propios titulares desconocen y que se efectúan sin ningún tipo de control y valiéndose de los vacíos de la legislación actual.

b) El caso conocido como “FARO”, en el que el Ministerio de Educación Pública recolectó datos personales sensibles relativos a la condición socioeconómica de menores de edad, sin el consentimiento de sus padres y violentando la privacidad de esos menores y sus familias.

c) Más recientemente, los ataques cibernéticos sufridos por los sistemas informáticos del Ministerio de Hacienda y otras entidades públicas por parte de cibercriminales. Se trata de la crisis de ciberseguridad más importante en la historia del país, gracias a la cual se expusieron datos personales de la ciudadanía, con las nefastas consecuencias de dicha filtración para la privacidad, patrimonio e integridad de los costarricenses.

Estas circunstancias evidencian la necesidad de poner límites y exigencias claras al uso y transferencia de datos en el sector público, especialmente cuando se invoca la necesidad de utilizar los datos para el ejercicio de potestades públicas ó la prestación de servicios públicos. Este proyecto introduce reglas y protocolos claros al respecto para que el uso de datos en el sector público sea transparente, seguro y respetuoso de los derechos fundamentales de la ciudadanía.

Con esta nueva norma, Costa Rica contará con las herramientas más avanzadas en materia de protección de datos personales para hacer frente a los retos de una economía fundamentada principalmente en los datos, que urge que los Estados promulguen reglas claras y estandarizadas que permitan conciliar la importancia de los flujos transfronterizos de datos personales con unas garantías suficientemente amplias que garanticen el cumplimento de la protección de datos de los ciudadanos en un entorno de gran incertidumbre tecnológica, en donde desconocemos no sólo el impacto que algunas tecnologías ya existentes podrán llegar a tener (piénsese en la Inteligencia Artificial), sino también las tecnologías que no han sido todavía desarrolladas.

Pero una nueva legislación requiere un replanteamiento de la autoridad reguladora en la materia, motivo por el que se debe modificar sustancialmente las funciones, potestades y sobre todo el perfil de institución del regulador. PRODHAB ha afrontado una serie de retos desde su creación, dentro de los que destacan:

1. Una alta rotación en sus directores, quienes además carecían de formación sobre la materia, y, una vez adquirido un conocimiento básico sobre esta, abandonaron el cargo por diversas circunstancias.

2. Recursos humanos, económicos y tecnológicos muy limitados. PRODHAB cuenta con un modesto número de funcionarios, encargados del cumplimiento de una larga lista de potestades conferidas por ley. De todos estos funcionarios, pocos de ellos cuenta con un perfil enfocado en tecnología, por lo que, en la actualidad la institución es materialmente incapaz de conducir, por ejemplo, una auditoría informática en los sistemas de un responsable del tratamiento.

3. La Agencia no ha contado con independencia de criterio; pues durante muchos años sus resoluciones eran remitidas en apelación al Despacho del Ministro de Justicia, el cual, a la hora de resolver, empleaba criterios no necesariamente técnicos, esto llevó a que algunas sanciones impuestas resultaran siendo revocadas en dicha instancia. Esta ausencia de independencia se vio reflejada también en los mencionados casos UPAD y FARO.

4. La dependencia de la Agencia del Ministerio de Justicia y Paz no tiene una justificación técnica, sobre todo porque se trata de un Ministerio que no tiene visibilidad sobre los temas vinculados con la tecnología. Lo más razonable es que la Agencia esté adscrita al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, como órgano especializado y rector del Poder Ejecutivo en todo lo relacionado con este tema.

5. A la ausencia de recursos humanos se suma la imposibilidad jurídica de la Agencia de imponer multas a los infractores de las disposiciones de la Ley, dada la inexistencia de un procedimiento administrativo aplicable, lo cual implica adoptar una reforma al Reglamento respectivo. Esto resulta indispensable para que la Agencia garantice el cumplimiento de la Ley 8968 y adicionalmente, para obtener los recursos derivados de la imposición de tales sanciones.

Los elementos que han sido tomados en consideración para el replanteamiento de Agencia de Protección de Datos, en la línea de las disposiciones del Convenio 108 de la Unión Europea y su Protocolo (Conocido como Convenio 108 plus), al cual Costa Rica ha aspira a adherirse en un futuro cercano, así como los Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos Personales, son las siguientes:

1. Plena autonomía en sus funciones.

2. Imparcialidad e independencia en sus potestades; por lo tanto, debe operar ajena de toda influencia externa, directa o indirecta, sin admitir orden ni instrucción alguna.

3. La dirección de la Agencia debe ser ocupada por una persona con experiencia y aptitudes en materia de protección de datos personales, y, al mismo

tiempo, debe ser nombrado mediante un procedimiento transparente y únicamente podrá ser removido de su cargo por causas graves, conforme a las reglas del debido proceso.

4. Deberá contar con suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros necesarios para garantizar el cumplimiento de la legislación y el respeto efectivo del derecho a la protección de datos personales.

5. Las resoluciones de la Dirección de la Agencia únicamente estarán sujetas al control jurisdiccional.

6. La Agencia deberá contar con los recursos humanos y materiales necesarios e idóneos para el cumplimiento de sus funciones. Debe haber, por ejemplo, personal experto en informática, ciencia de datos y nuevas tecnologías. En cuanto a su presupuesto, como garantía de independencia, la Agencia deberá proceder a su elaboración, sin injerencia del jerarca de la institución mediante la cual se relacione con la Administración (ministerio).

En consecuencia, la nueva Agencia de Protección de Datos Personales debe gozar de la estructura, la autonomía y la competencia que le habilite a ser un órgano en grado de desconcentración máxima, con una idoneidad especial y técnica que se relacione con la Administración mediante el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) , dotada de independencia administrativa, financiera y la potestad legalmente otorgada de dictar reglamentaciones específicas en la materia de su especialidad.

Asimismo, debe tener personalidad jurídica instrumental, para que le permita celebrar todo tipo de contratos y convenios con entidades públicas o privadas, tanto a nivel nacional como internacional. Su competencia también debe abarcar facultades plenas para conocer y resolver, ya sea por medio de denuncias o de oficio, así como sancionar, en caso de decidirlo discrecionalmente, toda conducta material o formal que configure una violación de los derechos de las personas frente a sus datos personales. Sus decisiones, darían por agotada la vía administrativa, sin que pudieran impugnarse las resoluciones frente al Ministerio, ni avocadas sus competencias.

Su unidad administrativa superior, deberá estar investida en la figura de un funcionario director, cuya idoneidad especial para la realización de su cargo exija la elección a través de un procedimiento de concurso público de doble control, es decir, nombrado por el Poder Ejecutivo y ratificado por el Poder Legislativo, lo cual garantiza una mayor legitimidad y obliga a una elección objetiva de una figura imparcial. Este funcionario director o funcionaria directora solo podrá ser removido por causales graves previamente establecidas en el ordenamiento jurídico, en concordancia con las normas del debido procedimiento.

La Agencia debe tener competencias para sancionar a todo responsable o encargado del tratamiento con una advertencia, cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en la normativa. Debe poder sancionar a todo responsable o encargado del tratamiento con apercibimiento, y ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos de los titulares de los datos.

Además, cuando proceda podrá ordenar al responsable o encargado del tratamiento que las operaciones se ajusten a la normativa vigente, de una determinada manera y dentro de un plazo especificado. También, ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales, imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición y hasta imponer una multa administrativa con arreglo a la normativa vigente en materia de protección de datos.

Estos aspectos implican un cambio en el sistema sancionatorio, para ello, cabe tener en cuenta, por ejemplo, la facturación o la pertenencia de la entidad a una estructura internacional, el riesgo para con los derechos de las personas o el impacto económico asociado al derecho vulnerado.

En ese sentido, el actual sistema sancionatorio y definición de posibles infracciones, así como su catalogación, debe ampliarse, según los requisitos normativos, derechos de las personas y la aplicación de nuevas tecnologías en el tratamiento de los datos.

En relación con el régimen sancionatorio, debe avanzarse dentro de las responsabilidades de cada entidad en el tratamiento de los datos, la adopción, no solo de sanciones tipificadas en virtud de su cuantía, sino en relación con el porcentaje de facturación, de acuerdo con el modelo sancionatorio introducido por el RGPDP.

Dicho porcentaje no se aplicaría con carácter exclusivo a la entidad infractora; sino en relación con la facturación del grupo al cual pertenece y siempre se tendrá en cuenta los tratamientos de datos, beneficios de su explotación e implementación de procedimientos y medidas a nivel grupo; por lo tanto, la sanción tendría un claro efecto disuasorio no solo a nivel local.

Esta Ley de Protección de Datos Personales marca un nuevo paradigma en materia de protección de datos personales no sólo en Costa Rica, sino en América Latina, siendo sin duda una de las normas más avanzadas y completas de la Región. La Ley refleja el estándar internacional en la materia, con una marcada influencia del RGPDP de la Unión Europea, su adaptación española en la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales, el Convenio 108 y sus Protocolos, algunas normas comparadas de la región como la Ley General de Protección de Datos de Brasil, y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, promulgados por la Red Iberoamericana de Protección de Datos Personales en el año 2017.

Es importante mencionar que, si bien existe en la corriente legislativa un proyecto de Ley (No. 22.388) que pretende reformar la Ley No. 8968 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, el proyecto contiene serias deficiencias, producto de la gran cantidad de enmiendas que tuvo durante el proceso, lo que lo convierte en un texto que no guarda coherencia. Además, la propuesta mantiene reglas de la ley actual que no han tenido ninguna incidencia en la práctica, como la obligación de registrar bases de datos ante la PRODHAB y pagar cánones por ello, lo cual, además de ser un trámite burocrático innecesario e injustificado, incrementa gravemente el riesgo de un ataque de ciberseguridad, al mantenerse una gran cantidad de datos de empresas y entidades públicas en los sistemas de PRODHAB, que claramente no tendrán el mismo grado de protección.

Pero sobre todo, el Proyecto 22.388 no contiene reglas suficientes para el uso y transferencia de datos en el sector público, ni establece sanciones claras para los supuestos en que el infractor sea un ente o funcionarios público, lo cual resta equilibrio al proyecto y no protege de las apuntadas negligencias que se han dado en el sector público en los últimos años. El presente proyecto guarda un mayor rigor técnico, regula otros supuestos de tratamientos de datos especialmente relevantes, y se encuentra contextualizado a la realidad y necesidades locales.

Este Proyecto consta de ochenta y tres artículos estructurados en diez capítulos, y así como cuatro disposiciones transitorias.

El Capítulo I, relativo a las disposiciones generales, comienza regulando el objeto de la Ley. Destaca en este Capítulo la novedosa regulación de los datos referidos a las personas fallecidas, excluyendo su tratamiento del ámbito de aplicación de la norma pero garantizando a las personas vinculadas al fallecido o a sus herederos el ejercicio de determinados derechos como el acceso, rectificación y supresión, en su caso con sujeción a las instrucciones del fallecido.

Los artículos 7 y 8 resultan fundamentales para garantizar que cualquier limitación al derecho de protección de datos personales deberá estar no sólo fundamentada en una ley especial, sino los requisitos mínimos que esta legislación deberá contemplar para asegurar garantías adecuadas al titular de los datos personales y conciliar el derecho a la protección de datos personales con otros derechos y libertades fundamentales.

Se introducen también reglas claras para la transferencia de datos entre instituciones públicas, de manera que, si no hay una ley expresa que faculte dicha transferencia pero ésta se entiende como implícitamente necesaria para alcanzar una finalidad pública dispuesta por Ley, la transferencia deba ser autorizada previamente por PRODHAB, y cumplir con una serie de requisitos legales concretos. Estas transferencias deben ser comunicadas a los titulares de los datos involucrados. Además, se prohíben las transferencias masivas e indiscriminadas de bases de datos completas, porque con esas transferencias masivas se incrementan

los riesgos de ciberseguridad y se violentan los principos de minimización y proporcionalidad.

En el Capítulo II se regulan los Principios de Protección de Datos Personales, recogiendo por primera vez en el ordenamiento jurídico costarricense el abanico completo de Principios aplicables a la materia: exactitud, legitimación, lealtad, transparencia, finalidad, minimización, calidad, responsabilidad, seguridad y confidencialidad. Se regula con especial detalle la figura del consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo la posibilidad de un consentimiento tácito, se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se regula específicamente el consentimiento por parte de menores de edad, fijando en quince años la edad a partir de la cual el menor puede prestar su consentimiento.

Se rompe finalmente el paradigma del tratamiento con el consentimiento como única base de legitimación, ampliando expresamente las bases de tratamiento al estándar internacional, incluyendo el cumplimiento de una obligación legal, la ejecución de un contrato, la protección de intereses vitales o la satisfacción de intereses legítimos.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, cuando derive de una competencia atribuida por la ley.

En cuanto a seguridad informática, se exige a los responsables adoptar en todo momento medidas de seguridad robustas y proporcionales al riesgo del tratamiento de los datos, con medidas como la pseudonimización o el cifrado de los datos, de manera que ante una vulneración de seguridad o ataque cibernético, no se comprometa la confidencialidad de los datos. Estas medidas deben ser constantemente revisadas, actualizadas y puestas a prueba por los responsables y encargados de los datos. Se aclara que las entidades públicas no podrán desaplicar o limitar el Principio de Seguridad bajo ninguna circunstancia, ni siquiera invocando el interés público.

El Capítulo III, dedicado a los derechos del titular, incluye por primera vez el elenco completo de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), y se incluye la novedosa figura del derecho a la portabilidad de los datos. Resalta la regulación del derecho de cancelación, también denominado derecho al olvido, estableciendo los supuestos en los cuales se podrá ejercer, pero también una serie de casos en los cuales dicho derecho no podrá ser ejercido, destacando por ejemplo el derecho a la libertad de expresión e información, con lo que se zanja la tensión existente entre los derechos fundamentales a la protección de datos y a la libertad de expresión, prevaleciendo este último.

Asimismo, se garantiza el derecho de todo titular a no ser objeto de decisiones individuales automatizadas basadas en sus datos, y a requerir la intervención humana, lo cual resulta esencial en un contexto en donde se aplican cada día con mayor frecuencia aplicaciones de inteligencia artificial para la toma de decisiones que tienen un impacto significativo en la vida de las personas.

En el Capítulo IV se refiere al responsable y al encargado del tratamiento. Se sigue el modelo internacional del RGPDP basado, fundamentalmente, en el principio de responsabilidad activa, que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Se introduce asimismo la figura de los corresponsables del tratamiento de datos personales.

Se migra del modelo regulatorio ex ante del registro de bases de datos, que en Costa Rica ha tenido una incidencia mínima, al modelo regulatorio ex post, basado en la responsabilidad activa del responsable, aplicando la figura del registro de actividades de tratamiento, que todo responsable deberá llevar y tener a disposición de la autoridad reguladora. Con la finalidad de no sobrecargar con costos y requisitos a las PYMES, en los casos en que el tratamiento de los datos no represente un riesgo a los derechos y libertades de los ciudadanos, se excluye de dicho deber de mantener un registro de actividades de tratamiento a las empresas con menos de 50 empleados, que se encuentren registradas como PYMES ante el Ministerio de Economía.

En el Capítulo V se regulan las transferencias internacionales de datos personales, y se refiere los supuestos en los cuales un responsable podrá realizar estas transferencias, replicando el estándar internacional en la materia no sólo en el RGPD sino también en el Convenio 108+, de forma igualmente compatible con las Directrices de la OCDE en la materia.

En el Capítulo VI se regulan las medidas proactivas en el tratamiento de datos personales, incluyendo figuras como la privacidad por diseño y privacidad por defecto y los mecanismos de autoregulación. Resalta en especial la figura del oficial de protección de datos, que adquiere una destacada importancia, y parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. Se determina que es obligatorio en determinadas actividades que entrañan un alto riesgo a los derechos y libertades de los titulares. La designación del oficial de protección de datos deberá de reportarse a la Agencia de Protección de Datos. Es de destacar que el oficial de protección de datos permite configurar un medio para la resolución amistosa de reclamos, pues el interesado podrá presentar ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

Por último, se regula la evaluación de impacto a la protección de datos como medida proactiva cuando el responsable pretenda llevar a cabo determinados tratamientos que por su naturaleza, alcance, contexto o finalidades entreñen un alto riesgo de afectación del derecho de protección de datos personales.

El Capítulo VII recoge Disposiciones aplicables a tratamientos concretos, incorporando una serie de supuestos de tratamientos lícitos cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto. Dentro de ellos se incluyen la videovigilancia, la geolocalización en el ámbito laboral, los sistemas de información crediticia (burós de crédito), la investigación en salud, y el tratamiento de datos personales para fines electorales. Por su especial incidencia y afectación sobre los Derechos Humanos de las personas, siguiendo las recomendaciones de las Naciones Unidas al respecto, y en apego a la cultura de protección a los Derechos Humanos de que goza Costa Rica, se establece una prohibición al uso de tecnologías de reconocimiento facial en espacios públicos, sin perjuicio de que el legislador pueda eventualmente reformar esta prohibición para permitir su uso en casos excepcionales de seguridad.

Se incluye una norma sobre el derecho de rectificación en Internet, que parte del reconocimiento del derecho a la libertad de expresión en Internet, con el detalle de un procedimiento para garantizar el derecho a rectificar una publicación digital que atente contra el honor o la intimidad de un titular, mediante la colocación de un aviso aclaratorio junto con la noticia original, lo cual permite conciliar ambos derechos.

El Capítulo VIII incluye un replanteamiento completo de la autoridad de protección de datos, mediante una autoridad administrativa independiente que se relaciona con la Administración a través del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. Se considera esencial un replanteamiento completo de la Agencia, cambiándole incluso su nombre, ampliando sus potestades y funciones y garantizándole independencia no sólo dándole la posibilidad de resolver los asuntos agotando la vía administrativa, dictando reglamentos a la Ley y aprobando su propio presupuesto, sino también mediante un procedimiento de designación de su Dirección que parta de un concurso público de antecedentes, con doble control, y que además, una vez designada, sólo pueda ser destituida por falta grave a sus obligaciones.

Resulta indispensable garantizar que la Agencia de Protección de Datos gozará de los recursos humanos y económicos para el desarrollo de sus competencias, ya que la Ley, para cumplir su cometido, parte de la existencia de una autoridad reguladora relevante que asuma una rectoría en materia de protección de datos en el país. Las competencias y potestades que se le garantizan en la Ley no pueden cumplirse sin una adecuada estructura administrativa y funcionarios competentes y cualificados.

El Capítulo IX regula el Procedimientos en caso de posible vulneración de la normativa de protección de datos. La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia de

Protección de Datos remita la reclamación al oficial de protección de datos; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos.

El Capítulo X contempla el régimen sancionador, que incluye un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. La Ley incluye un elenco de conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, a efectos de fijar la cuantía de las sanciones y sus plazos de prescripción.

En cuanto a las sanciones, se incrementa su cuantía económica con respecto a la Ley 8968, que establecía unas sanciones económicas lo suficientemente modestas como para que no alentaran la adaptación de las empresas a la norma. Asimismo, se determina un régimen sancionatorio diferenciado para determinados organismos públicos. Se incluyen una serie de criterios que permiten valorar las circunstancias de cada caso individual para efectos de imponer sanciones y medidas correctivas.

Finalmente, el Capítulo XI de esta Ley establece el derecho del titular a la reparación del daño sufrido producto de una violación de su derecho a la protección de datos personales, mismo que deberá ser ejercido en la vía judicial, fijándose un plazo de prescripción de un año.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DECRETA:

LEY DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1- Objeto

1. La presente Ley tiene por objeto:

a. Establecer un conjunto de principios y derechos de protección de datos personales con la finalidad de garantizar un debido tratamiento de los datos personales de los habitantes.

b. Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

c. Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.

d. Facilitar el flujo internacional de los datos personales, con la finalidad de coadyuvar al crecimiento social y económico de la región.

e. Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia.

ARTÍCULO 2- Definiciones

1. Para los efectos de la presente Ley se entenderá por:

a. Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.

b. Base de datos: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado.

c. Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del titular.

d. Consentimiento: manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza mediante una acción declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.

e. Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

f. Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

g. Datos personales: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

h. Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

i. Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

j. Encargado: prestador de servicios, que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.

k. Exportador: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en esta Ley.

l. Fuentes de acceso público: bases de datos públicas que pueden ser accedidas por cualquier persona, siempre y cuando una ley especial les haya dado

ese carácter de manera expresa, o dicho acceso público sea razonablemente necesario para cumplir los fines previstos en esa ley especial y para los cuales se conformó la base de datos. Se entienden como fuentes de acceso público, entre otras que puedan existir, las bases de datos de personas jurídicas, bienes inmuebles, bienes muebles, catastro y propiedad industrial del Registro Nacional, los registros de nacimientos, matrimonios y defunciones del Registro Civil, y las bases de datos que acrediten la condición de colegiado a un colegio profesional.

m. Grupo empresarial: grupo constituido por una empresa que ejerce el control y sus empresas controladas.

n. Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

o. Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento para transferencias, cesiones o un conjunto de transferencias y cesiones de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

p. Responsable: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

q. Seudoanonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

r. Sistema de identificación biométrica: sistema o software que se desarrolla empleando: a) estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado, el realizado por refuerzo, o el aprendizaje automático; b) estrategias basadas en la lógica y el conocimiento; o c) estrategias estadísticas y análogas; destinado a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada. Se entenderá que se utiliza un sistema de identificación biométrica “en tiempo real” cuando la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Este término engloba no solo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión.

s. Tercero: persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del Responsable, Encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

t. Titular: persona física a quien le conciernen los datos personales.

u. Transferencia de datos: se refiere a la transmisión o entrega de datos personales o bases de datos de un responsable o encargado del tratamiento a un nuevo responsable o corresponsable del tratamiento, que podrá definir de forma independiente o conjunta las finalidades y medios del tratamiento de los datos recibidos.

v. Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

ARTÍCULO 3- Ámbito de aplicación subjetivo

Esta Ley será aplicable a las personas físicas o jurídicas de carácter privado, y a la administración pública centralizada y descentralizada, que realicen tratamiento de datos personales en el ejercicio de sus actividades y funciones.

ARTÍCULO 4- Ámbito de aplicación objetivo

1. Esta Ley será aplicable al tratamiento de datos personales de personas físicas que consten o estén destinados a constar en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

2. Esta Ley no será aplicable en los siguientes supuestos:

a. Cuando los datos personales estén destinados exclusivamente a actividades en el marco de la vida familiar o doméstica de una persona física, esto es, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito una divulgación o utilización comercial.

b. La información anónima, es decir, aquélla que no guarda relación con una persona física identificada o identificable, así como los datos personales sometidos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado.

c. A los tratamientos de persona fallecidas, sin perjuicio de lo establecido en el artículo 5 de esta Ley.

d. A los tratamientos sometidos a la normativa sobre protección de materias clasificadas o secretos de Estado.

ARTÍCULO 5- Datos de personas fallecidas

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento con objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

2. Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente por escrito o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

3. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

4. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales.

5. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de salvaguardia, si tales facultades se entendieran comprendidas en las medidas de salvaguardia prestadas por el designado.

ARTÍCULO 6- Ámbito de aplicación territorial

1. Esta Ley resultará aplicable al tratamiento de datos personales efectuado:

a. Por un responsable o encargado con establecimiento en la República de Costa Rica.

b. Por un responsable o encargado sin establecimiento en la República de Costa Rica, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los habitantes de la República de Costa Rica, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en la República de Costa Rica.

c. Por un responsable o encargado que no cuente con establecimiento en la República de Costa Rica, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud de las normas del derecho internacional privado.

d. Por un responsable o encargado sin establecimiento en territorio costarricense y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.

2. Para los efectos de la presente Ley, se entenderá por establecimiento el lugar de la administración central o principal del responsable o encargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento de datos personales que lleve a cabo, a través de modalidades estables.

3. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituirán, en sí mismas, un establecimiento principal y no serán considerados como criterios determinantes para la definición del establecimiento principal del responsable o encargado.

4. Cuando el tratamiento de datos personales lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo.

ARTÍCULO 7- Excepciones generales al derecho a la protección de datos personales

1. Cualquier ley que tenga como propósito limitar el derecho a la protección de datos personales contendrá, como mínimo, disposiciones relativas a:

a. La finalidad del tratamiento.

b. Las categorías de datos personales de que se trate.

c. El alcance de las limitaciones establecidas.

d. Las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas.

e. La determinación del responsable o responsables.

f. Los plazos de conservación de los datos personales.

g. Los posibles riesgos para los derechos y libertades de los titulares.

h. El derecho de los titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta.

2. Las leyes serán las necesarias, adecuadas y proporcionales en una sociedad democrática, y deberán respetar los derechos y las libertades fundamentales de los titulares.

3. Ninguna limitación del derecho fundamental a la protección de datos personales podrá vaciar de contenido este derecho, por lo que se respetará el cumplimiento de las garantías, principios y derechos del titular que no sea necesario limitar o restringir para acometer el fin público perseguido. El deber de información deberá ser garantizado en todo momento. El incumplimiento de este inciso dará pie a responsabilidad disciplinaria de los funcionarios implicados y a responsabilidad administrativa del Estado, sin perjuicio de las demás sanciones previstas en el régimen sancionatorio de esta Ley o de las responsabilidades penales establecidas en el Código Penal.

ARTÍCULO 8- Tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y transferencias interinstitucionales

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable cuando así lo prevea una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras similares.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable cuando derive de una competencia atribuida por una norma con rango de ley.

3. Las transferencias de datos personales que se efectúen entre entes públicos en el marco de una obligación legal, interés público o ejercicio de poderes públicos, así como todo tratamiento realizado con los datos transferidos, serán lícitas en la medida en que se cumplan las siguientes condiciones acumulativas:

a) Que una ley especial lo autorice expresamente, o que la transferencia sea estrictamente necesaria para cumplir con los fines de interés público asignados por Ley a la entidad receptora de los datos. En el caso de esta segunda alternativa, la transferencia solo se llevará a cabo previa autorización de la Agencia de Protección de Datos, quien deberá verificar que:

i) la transferencia sea absolutamente necesaria para cumplir con el fin público invocado y asignado por Ley a la entidad receptora;

ii) que los datos a ceder son los estrictamente necesarios y adecuados para ese fin.

iii) que la entidad receptora de los datos cuenta con las medidas de seguridad, protocolos y demás garantías establecidas en esta Ley, para proteger la integridad, disponibilidad y confidencialidad de los datos.

b) Que el ente que transfiere los datos los haya obtenido con fundamento en una de las bases legales previstas en el artículo 14 y en el ejercicio de sus competencias asignadas por ley.

c) Que el ente receptor utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de sus competencias legales vigentes.

d) Que los datos involucrados en la transferencia sean únicamente los adecuados y estrictamente necesarios para acometer la finalidad pública, de conformidad con el principio de minimización. Se prohíbe la cesión masiva e indiscriminada de bases de datos.

En cualquiera de los anteriores supuestos, las transferencias deberán ponerse en conocimiento de todos los titulares de los datos involucrados de manera segura y sin comprometer su confidencialidad, dentro de los siguientes quince días a la ejecución de la transferencia. Además, la transferencia debe documentarse en un convenio interinstitucional que deberá ser publicado y puesto a disposición de la ciudadanía para su escrutinio, resguardando la confidencialidad de los datos personales involucrados en la transferencia. Este convenio deberá contener disposiciones específicas respecto de las condiciones que rigen la licitud del tratamiento por parte de las personas responsables; la descripción clara de la categoría de personas cuyos datos se procesarán, sin exponer datos que puedan identificar a las personas; los tipos de datos objeto de tratamiento, especialmente si contienen categorías de datos sensibles; la finalidad específica del tratamiento; los plazos de conservación de los datos; un detalle de las operaciones y los procedimientos del tratamiento; incluidas las medidas técnicas, físicas y organizativas de seguridad que se establecerán para proteger la información; y un medio de contacto para obtener más información sobre la transferencia.

Las transferencias no serán de conocimiento público ni deberán ser puestas en conocimiento de los titulares cuando tengan por objeto la investigación de un posible delito o para fines policiales, ni en aquellos casos donde la revelación de la transferencia a los titulares pueda comprometer seriamente el objetivo de interés público perseguido con la transferencia.

ARTÍCULO 9- Tratamiento de datos personales de niñas, niños y adolescentes

1. En el tratamiento de datos personales concernientes a niñas, niños y adolescentes se privilegiará la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.

2. Se promoverá en la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.

3. Los padres, madres, tutores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

ARTÍCULO 10- Tratamiento de datos personales sensibles

1. Por regla general, queda prohibido el tratamiento de datos personales sensibles, que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, salvo que se presente cualquiera de los siguientes supuestos:

a. Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación.

b. Se dé cumplimiento a un mandato legal.

c. Sea necesario para proteger intereses vitales del titular o de otra persona física, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento;

d. Se cuente con el consentimiento expreso del titular con uno o más fines especificados.

e. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros, fundados en ley especial, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

f. Sea necesarios para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación aplicable a la materia o en virtud de un contrato con un profesional de la salud sujeto a la obligación de secreto profesional, o bajo su responsabilidad.

g. Sean necesarios por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, con fundamento en una legislación que establezca medidas adecuadas y específicas para proteger los derechos y libertades del titular, en particular el secreto profesional,

h. Sean con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, con fundamento en una ley especial que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

2. Exclusivamente mediante ley aplicable en la materia podrá establecerse excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles.

ARTÍCULO 11- Tratamiento de datos personales relativos a condenas e infracciones penales

1. El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas. Solo podrá llevarse un registro completo de condenas penales bajo el control del Poder Judicial.

ARTÍCULO 12- Tratamiento de datos personales obtenidos de fuentes de acceso público

Los datos obtenidos de fuentes de acceso público solo podrán ser tratados para los fines establecidos por Ley, y de conformidad con el principio de minimización, por lo que solo serán incluidos en estas bases los datos estrictamente necesarios,

adecuados y pertinentes para cumplir la finalidad pública. Los titulares gozarán de todos los derechos, principios y garantías establecidos en esta Ley respecto de sus datos personales que consten en fuentes de acceso público, los cuales solo podrán ser limitados, mas no extinguidos, en la medida en que la limitación sea estrictamente necesaria, idónea y proporcional para garantizar los fines de interés público de la base de datos pública.

Bajo ninguna circunstancia un dato personal sensible podrá ser incorporado en una base de datos de acceso público.

CAPÍTULO II
PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 13- Principios aplicables al tratamiento de datos personales

1. En el tratamiento de datos personales, el responsable observará los principios de exactitud, legitimación, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

ARTÍCULO 14- Principio de exactitud

1. Los datos serán exactos, y si fuere necesario, actualizados. No será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a. Hubiesen sido obtenidos por el responsable directamente del afectado.

b. Hubiesen sido obtenidos por el responsable de un encargado que los recogió en nombre propio para su transmisión al responsable.

c. Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio del afectado del derecho a la portabilidad previsto en esta Ley.

d. Fuesen obtenidos de un registro público por el responsable.

ARTÍCULO 15- Principio de legitimación

1. El responsable solo podrá tratar datos personales cuando se presente alguno de los siguientes supuestos:

a. El titular otorgue su consentimiento para una o varias finalidades específicas.

b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente.

c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una habilitación legal.

d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.

e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte.

f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.

g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física.

h. El tratamiento sea necesario por razones de interés público establecidas o previstas en ley.

i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones.

2. Tratándose de este último inciso, se entenderá amparado por el interés legítimo el tratamiento de datos personales de contacto que sea imprescindible para la localización de personas físicas que prestan sus servicios al responsable, con la finalidad de mantener cualquier tipo de relación con ésta.

3. El tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que la ley les confiera expresamente.

ARTÍCULO 16- Condiciones para el consentimiento

1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente Ley.

4. No podrá supeditarse la ejecución de un contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

5. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos. La revocación del consentimiento no afectará la licitud del tratamiento basada en el consentimiento previo a su revocación.

6. Cuando los datos y/o el consentimiento se recaben a través de internet, aplicaciones móviles u otros medios electrónicos, el responsable podrá cumplir su deber de información en capas, suministrando al interesado, en la misma sección donde se recolecta el consentimiento, un vínculo funcional que remita al interesado al sitio donde almacena el responsable la información exigida en el artículo 6 de esta Ley.

ARTÍCULO 17- Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de quince años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de quince años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, conforme lo previsto en la legislación respectiva.

ARTÍCULO 18- Principio de lealtad

1. El responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos.

2. Para los efectos de esta Ley, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares.

ARTÍCULO 19- Principio de transparencia

1. Cuando se obtengan directamente de un titular, datos personales relativos a él, el responsable informará al titular en el momento en que estos se obtengan sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

2. El responsable proporcionará al titular, al menos, la siguiente información:

a. Su identidad y datos de contacto.

b. Los datos de contacto del oficial de protección de datos, de haberlo.

c. Las finalidades del tratamiento a que serán sometidos sus datos personales y la base jurídica del tratamiento.

d. Las transferencias, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas.

e. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

f. El plazo durante el cual se conservarán los datos personales, o cuando no sea posible, los criterios utilizados para determinar ese plazo.

g. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

h. El derecho del titular a presentar una reclamación ante la Agencia de Protección de Datos.

3. La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes.

4. Cuando los datos sean obtenidos del titular, el responsable del tratamiento podrá dar cumplimiento al deber de información facilitando al titular la información básica contenida en los incisos a, b y d del inciso 2 de este artículo, e indicándole una dirección electrónica o proporcionándole un vínculo funcional u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

5. Todo responsable contará con políticas transparentes de los tratamientos de datos personales que realice.

ARTÍCULO 20- Principio de finalidad

1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.

2. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

3. El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

ARTÍCULO 21- Principio de minimización

1- El responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

ARTÍCULO 22- Principio de calidad

1- El responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

2- Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

3- En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.

4- Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable. No obstante, la ley podrá establecer excepciones respecto al plazo de conservación de los datos personales, con pleno respeto a los derechos y garantías del titular.

ARTÍCULO 23- Principio de responsabilidad

1. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en esta Ley, así como

rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la Agencia de Protección de Datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

2. Lo anterior, aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.

3. Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.

b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.

c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

4. El responsable revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

ARTÍCULO 24- Principio de seguridad

1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

2. Para la determinación de las medidas referidas en el numeral anterior, el responsable considerará los siguientes factores:

a. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

b. El estado de la técnica.

c. Los costos de aplicación.

d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.

e. El alcance, contexto y las finalidades del tratamiento.

f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.

g. El número de titulares.

h. Las posibles consecuencias que se derivarían de una vulneración para los titulares.

i. Las vulneraciones previas ocurridas en el tratamiento de datos personales.

3. El responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica, para garantizar un nivel de seguridad adecuado al riesgo, que podrá incluir entre otros:

a. La seudonimización y el cifrado de los datos personales.

b. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resilencia permanentes de los sistemas y servicios de tratamiento.

c. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos

siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud de disposición legal aplicable.

5. Bajo ninguna circunstancia podrá una entidad u órgano de la Administración Pública o del Estado, invocando el ejercicio de potestades públicas o la satisfacción de intereses públicos, desaplicar o limitar el principio de seguridad aquí descrito.

6. Sin perjuicio de las obligaciones y medidas impuestas en este artículo, la Agencia de Protección de Datos establecerá un estándar mínimo de ciberseguridad para el sector público, o acordará adoptar alguno ya existente en la materia, el cual será de acatamiento obligatorio para la totalidad de la Administración Pública. El cumplimiento del estándar mínimo no exime a las entidades públicas de su obligación de disponer de mayores medidas de seguridad en función de los criterios establecidos en el inciso 2 de este artículo y del nivel de riesgo aplicable a cada institución. El Reglamento a ésta Ley dispondrá las características, elementos y medidas técnicas, físicas y lógicas de ciberseguridad mínimas que deberán cumplir las entidades públicas, el mecanismo de control que se utilizará para verificar el cumplimiento de dicho estándar, y la periodicidad con que deberá demostrarse dicho cumplimiento.

ARTÍCULO 25- Notificación de vulneraciones a la seguridad de los datos personales

1. Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales, aún cuando ocurra de manera accidental, notificará a la Agencia de Protección de Datos Personales en un plazo de 72 horas, desde que se tuviera conocimiento efectivo y, a los titulares afectados dicho acontecimiento, sin dilación alguna.

2. Lo anterior, no resultará aplicable cuando el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la vulneración de seguridad ocurrida, o bien, que ésta no represente un riesgo para los derechos y las libertades de los titulares involucrados.

3. La notificación que realice el responsable a los titulares afectados estará redactada en un lenguaje claro y sencillo, posibilitando acreditar el envío de la notificación referida.

4. La notificación a que se refieren los numerales anteriores contendrá, al menos, la siguiente información:

a. La naturaleza del incidente.

b. Los datos personales comprometidos.

c. Las acciones correctivas realizadas de forma inmediata.

d. Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses.

e. Los medios disponibles al titular para obtener mayor información al respecto.

4. Cuando por la gravedad o naturaleza particular del incidente sea imposible identificar todos los elementos anteriores dentro de las 72 horas establecidas en el inciso primero, el responsable deberá notificar la información de la que tenga conocimiento a ese momento, debiendo completar y notificar el resto de la información indicada en un plazo no mayor a cinco días hábiles desde que haya tenido conocimiento del incidente.

5. El responsable auditará y documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la vulneración; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la Agencia de Protección de Datos.

6. El reglamento que se dicte a la presente ley establecerá los efectos de las notificaciones de vulneraciones de seguridad que realice el responsable a la autoridad de control, en lo que se refiere a los procedimientos, forma y condiciones de su intervención, con el propósito del salvaguardar los intereses, derechos y libertades de los titulares afectados.

ARTÍCULO 26- Principio de confidencialidad

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad. Este deber será complementario de los deberes de secreto profesional de conformidad con la normativa aplicable.

2. El responsable o encargado establecerán controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular.

CAPÍTULO III
DERECHOS DEL TITULAR

ARTÍCULO 27- Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y de portabilidad

1. En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen.

2. El ejercicio de cualquiera de los derechos referidos en el numeral anterior no es requisito previo, ni impide el ejercicio de otro.

ARTÍCULO 28- Disposiciones generales sobre ejercicio de los derechos

1. Los derechos reconocidos en en este Capítulo, podrán ejercerse directamente o por medio de representante legal o voluntario, debiendo estar estos debidamente acreditados. Cuando el responsable tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de quince años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente Ley.

6. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos.

ARTÍCULO 29- Derecho de acceso

1.- El titular tendrá derecho a obtener del responsable del tratamiento 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 siguiente información:

a. Los fines del tratamiento.

b. Las categorías de datos personales de que se trate.

c. Los destinatarios o las categorías de destinatarios a los que se transfirieron o serán transferidos los datos personales, en particular destinatarios en terceros países u organizaciones internacionales.

d. De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.

e. La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al titular, o a oponerse a dicho tratamiento.

f. Cuando los datos personales no se hayan obtenido del titular, cualquier información disponible sobre su origen.

2. Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

3. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

4. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el titular un canon razonable basado en los costos administrativos. Cuando el titular presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

5. Se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello. En dicho caso, el responsable podrá denegar la solicitud por ese motivo hasta que transcurra dicho plazo.

ARTÍCULO 30- Derecho de rectificación

1. El titular tendrá el derecho a obtener del responsable, en el plazo máximo de cinco días hábiles, la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados. Al ejercer este derecho el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la

documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

ARTÍCULO 31- Derecho de cancelación (derecho al olvido)

1. El titular tendrá derecho a obtener del responsable del tratamiento y en el plazo de cinco días hábiles, la cancelación de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

b. El titular retire el consentimiento en que se basa el tratamiento, y este no se base en otro fundamento jurídico.

c. El titular se oponga al tratamiento con arreglo al artículo 32 apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el titular se oponga al tratamiento con arreglo al artículo 32, apartado 2.

d. Los datos personales hayan sido tratados ilícitamente.

e. Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en una ley especial que se aplique al responsable del tratamiento.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el costo de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales, de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a. Para ejercer el derecho a la libertad de expresión e información.

b. Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por ley especial que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

c. Por razones de interés público en el ámbito de la salud pública.

d. Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho indicado en el apartado

1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.

e. Para la formulación, el ejercicio o la defensa de reclamaciones.

ARTÍCULO 32- Derecho de oposición

1. El titular podrá oponerse en cualquier momento al tratamiento de sus datos personales, cuando dicho tratamiento se fundamente en las causales de los incisos h) e i) del artículo 15 (1) de esta Ley, cuando:

a. Tenga una razón legítima derivada de su situación particular, misma que deberá justificar en su solicitud de oposición.

b. El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.

2. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.

3. Tratándose del inciso 1 (b) anterior, cuando el titular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines.

ARTÍCULO 33- Derecho a no ser objeto de decisiones individuales automatizadas

1. El titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa, que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

2. Lo dispuesto en el numeral anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable o bien, se base en el consentimiento demostrable del titular.

3. No obstante, cuando el tratamiento automatizado sea necesario para la relación contractual o el titular hubiere manifestado su consentimiento, éste tendrá derecho a obtener una intervención humana significativa; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión.

4. El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, género, así como datos genéticos o datos biométricos.

ARTÍCULO 34- Derecho a la portabilidad de los datos personales

1. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.

3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

4. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

ARTÍCULO 35- Derecho a la limitación del tratamiento de los datos personales

1. El titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable.

2. El titular tendrá derecho a la limitación del tratamiento de sus datos personales cuando éstos sean innecesarios para el responsable, pero los necesite para formular una reclamación.

ARTÍCULO 36- Ejercicio de los derechos ARCO y de portabilidad

1. El responsable establecerá medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.

2. Por vía reglamentaria se establecerán los requerimientos, plazos, términos y condiciones en que los titulares podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad, así como las causales de

improcedencia al ejercicio de los mismos como podrían ser, de manera enunciativa más no limitativa:

a. Cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público.

b. Cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas.

c. Cuando el responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular.

d. Cuando el tratamiento sea necesario para el cumplimiento de una disposición legal.

e. Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

3. Cuando las solicitudes de ejercicio de derechos sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable podrá:

a. Cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada.

b. Negarse a actuar respecto de la solicitud.

4. En todo caso, el responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

CAPÍTULO IV
RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

ARTÍCULO 37- Obligaciones generales del responsable y encargado del tratamiento

1- Los responsables y encargados determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con la presente ley y sus normas de desarrollo. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos a que se refiere el artículo 51 de esta Ley.

2- Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a. Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b. Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c. Cuando se produjese el tratamiento no meramente incidental o accesorio de datos sensibles, en los términos que son definidos en esta Ley, o de los datos relacionados con la comisión de infracciones administrativas.

d. Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e. Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f. Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g. Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección por parte de la Agencia de Protección de Datos.

h. Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

ARTÍCULO 38- Corresponsables del tratamiento

1.- Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por la presente Ley, atendiendo a las actividades que efectivamente desarrolle cada

uno de los corresponsables del tratamiento, en particular en cuanto al ejercicio de los derechos del titular y a sus respectivas obligaciones de transparencia a que se refiere el artículo 19 de esta Ley. Dicho acuerdo podrá designar un punto de contacto para los titulares.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los titulares. Se pondrán a disposición del titular los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los titulares podrán ejercer los derechos que les reconoce la presente Ley frente a, y en contra de, cada uno de los responsables.

ARTÍCULO 39- Comunicaciones o cesiones de datos

1- Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2- El consentimiento exigido en el apartado anterior no será preciso:

a. Cuando la cesión está autorizada en una ley.

b. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con bases de datos de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

c. Cuando la comunicación que deba efectuarse tenga por destinatario al Ministerio Público, los Tribunales de Justicia o a la Controlaría General de la República, en el ejercicio de las funciones que tiene atribuidas.

d. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. Las cesiones entre administraciones públicas que impliquen transferencia de datos personales, seguirán las reglas establecidas en el artículo 8 de la presente Ley.

e. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a una base de datos o para realizar los estudios epidemiológicos en los términos establecidos en la legislación nacional sobre sanidad y salud pública.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le

permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

ARTÍCULO 40- Encargado de tratamiento

1. El encargado realizará las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el responsable.

2. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará transferencia de datos siempre que se cumpla lo establecido en la presente Ley y en sus normas de desarrollo.

3. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo siguiente. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público. Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

4. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

5.- El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

6.- En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración Pública, las municipalidades o instituciones descentralizadas, siempre que sea mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo siguiente.

ARTÍCULO 41- Formalización de la prestación de servicios del encargado

1. La prestación de servicios entre el responsable y encargado se formalizará mediante la suscripción de un contrato de encargo.

2. El contrato de encargo establecerá, al menos, el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento; el tipo de datos personales; las categorías de titulares, así como las obligaciones y responsabilidades del responsable y encargado.

3. El contrato o instrumento jurídico establecerá, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

a. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.

b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.

c. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

d. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.

e. Informar al responsable cuando un titular ejercite sus derechos en materia de protección de datos a través del encargado.

f. Guardar confidencialidad respecto de los datos personales tratados.

g. Suprimir, devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones de éste, excepto que una disposición legal exija la conservación de los datos personales, o bien, que el responsable autorice la comunicación de éstos a otro encargado.

h. Abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control.

i. Permitir al responsable o autoridad de control inspecciones y verificaciones en sitio. Estas verificaciones podrán hacerse a través de las certificaciones de seguridad de la información con las que cuente el encargado.

j. Generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones.

k. Colaborar con el responsable en todo lo relativo al cumplimiento de la legislación aplicable en la materia.

4. Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el alcance, contenido, medios y demás cuestiones del tratamiento de los datos personales asumirá la calidad de responsable.

ARTÍCULO 42- Subcontratación de servicios

1. El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del responsable, o bien, se estipule expresamente en el contrato o instrumento jurídico suscrito entre este último y el encargado.

2. El subcontratado asumirá el carácter de encargado.

3. El encargado formalizará la prestación de servicios del subcontratado a través de un contrato, debiendo aportar las garantías recogidas en el artículo 41 de la presente ley.

4. Cuando el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos personales que lleve a cabo conforme a lo instruido por el encargado, asumirá la calidad de responsable.

ARTÍCULO 43- Registro de actividades de tratamiento

1. Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a. El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del oficial de protección de datos.

b. Los fines del tratamiento.

c. Una descripción de las categorías de titulares y de las categorías de datos personales.

d. Las categorías de destinatarios a quienes se transfirieron o transferirán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.

e. En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 44, apartado 1, inciso d), la documentación de garantías adecuadas.

f. Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

g. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 24.

2. Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y del oficial de protección de datos, de haberlo.

b. Las categorías de tratamientos efectuados por cuenta de cada responsable.

c. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional.

d. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 24.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la Agencia de Protección de Datos cuando ésta lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 50 personas o se encuentre registrada y al día como PYME ante el Ministerio de Economía Industria y Comercio, , a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los titulares, no sea ocasional, o incluya datos sensibles.

ARTÍCULO 44- Bloqueo de los datos

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Público o las Administraciones Públicas competentes, en particular de la Agencia de Protección de Datos, para la exigencia

de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia de Protección de Datos podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO V
TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

ARTÍCULO 45- Reglas generales para las transferencias internacionales de datos personales

1. Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional, si el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán e interpretarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por la presente Ley no se vea menoscabado.

2. El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:

a. Cuando el responsable cuente con el consentimiento informado del titular de los datos.

b. Cuando la transferencia sea exigida legalmente o en un tratado internacional del que la República de Costa Rica sea parte, para la investigación y persecución de los delitos, así como la administración de justicia o por razones de seguridad nacional.

c. Cuando el país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte de la Agencia de Protección de Datos, o bien, el país destinatario acredite condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado.

d. Cuando el exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y acredite el cumplimiento de las condiciones mínimas y suficientes aplicables a la materia. Se considerarán como garantías suficientes las siguientes:

i) Que el exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes del cumplimiento de la presente Ley y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares.

ii) Que el exportador y destinatario adopten un esquema de autorregulación vinculante, normas corporativas vinculantes o un mecanismo de certificación, siempre y cuando éste sea acorde con las disposiciones previstas en esta Ley.

e. Que se encuentre prevista en una ley o tratado internacional del que la República de Costa Rica sea parte.

3. En todos los casos de transferencias regidas por el presente artículo, el acuerdo o mecanismo que instrumente la transferencia, deberá asegurar que el importador de los datos personales se encuentre sujeto a la jurisdicción de una o varias autoridades de supervisión independientes -tales como una autoridad de protección de datos y los tribunales que pudieran resultar competentes en el país de destino- de manera que los titulares o interesados cuenten con acciones legales efectivas -administrativas y judiciales- para proteger sus derechos. Asimismo, el acuerdo o mecanismo que instrumente la transferencia deberá reconocer que la parte exportadora se encuentra sujeta a la jurisdicción de la Agencia de Protección de Datos y de los tribunales de Costa Rica que resulten competentes.

CAPÍTULO VI

MEDIDAS PROACTIVAS EN EL TRATAMIENTO DE DATOS PERSONALES

ARTÍCULO 46- Reconocimiento de medidas proactivas

1- Se establecen como medidas que promueven el mejor cumplimiento de la legislación y que coadyuvan a fortalecer y elevar los controles de protección de datos personales implementados por el responsable, las que a continuación se indican en el presente Capítulo.

ARTÍCULO 47- Privacidad por diseño y privacidad por defecto

1. El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en esta Ley.

2. El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en esta Ley. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas.

ARTÍCULO 48- Oficial de protección de datos personales

1. El responsable designará a un oficial de protección de datos personales cuando se trate de las siguientes entidades:

a. Instituciones públicas de la administración central o descentralizada.

b. El Poder Judicial y el Tribunal Supremo de Elecciones.

c. Colegios profesionales.

d. Empresas de seguridad privada.

e. Los centros sanitarios que mantengan historias clínicas de los pacientes, exceptuando los profesionales de la salud que, aun manteniendo historias clínicas, ejerzan su actividad a título individual.

f. Entidades bancarias y financieras, sujetas a la regulación de la Superintendencia General de Entidades Financieras.

g. Las entidades responsables de bases de datos de evaluación de solvencia patrimonial y crédito.

h. Los responsables que lleven a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular.

i. Los responsables que realicen tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, considerando, entre otros factores y de manera enunciativa más no limitativa, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen; el número de titulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de éstos.

2. El responsable que no se encuentre en alguna de las causales previstas en el numeral anterior, podrá designar a un oficial de protección de datos personales si así lo estima conveniente.

3. Los responsables deberán informar en un plazo de diez días naturales a la Agencia de Protección de Datos las designaciones, nombramientos y ceses de los oficiales de protección de datos tanto en los supuestos en que se encuentren obligados a su designación como en el caso en que sea voluntaria.

4. Los oficiales de protección de datos podrán ejercer su función a tiempo completo o parcial, dependiendo del volumen de tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los titulares. El oficial de protección de datos podrá ser una persona física o jurídica, interna o externa a la organización, y deberá acreditar conocimientos especializados en el derecho y la práctica de protección de datos. La Agencia de Protección de Datos mantendrá una lista actualizada de los oficiales de protección de datos que será accesible por medios electrónicos.

5. El responsable estará obligado a respaldar al oficial de protección de datos personales en el desempeño de sus funciones, facilitándole los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos.

6. El oficial de protección de datos personales tendrá, al menos, las siguientes funciones:

a. Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.

b. Coordinar, al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación aplicable en la materia.

c. Supervisar al interior de la organización del responsable el cumplimiento de la legislación aplicable en la materia.

7. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el oficial de protección de datos no podrá ser removido ni sancionado por el responsable por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del oficial de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

8. En el ejercicio de sus funciones el oficial de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable la existencia de cualquier deber de confidencialidad o secreto.

9. Cuando el oficial de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable.

ARTÍCULO 49- Intervención del oficial de protección de datos en caso de reclamación ante la Agencia de Protección de Datos

1. Cuando el responsable hubiera designado un oficial de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquel ante la Agencia de Protección de Datos, dirigirse al oficial de protección de datos de la entidad contra la que se reclame.

En este caso, el oficial de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia de Protección de Datos esta podrá remitir la reclamación al oficial de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el oficial de protección de datos no hubiera comunicado a la Agencia de Protección de Datos la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en esta Ley y en sus normas de desarrollo.

ARTÍCULO 50- Mecanismos de autorregulación

1. El responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación de esta Ley y establecer procedimientos de resolución de

conflictos entre el responsable y titular, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del titular.

2. Para los efectos del numeral anterior, se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos señalados en el presente numeral.

3. La Agencia de Protección de Datos establecerá las reglas que correspondan para la validación, confirmación o reconocimiento de los mecanismos de autorregulación aludidos.

ARTÍCULO 51- Evaluación de impacto a la protección de datos personales

1.- Cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa a la implementación del mismo, una evaluación del impacto a la protección de los datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a. Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b. Tratamiento a gran escala de datos sensibles.

c. Observación sistemática a gran escala de una zona de acceso público.

4. La Agencia de Protección de Datos podrá promulgar una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos, asimismo podrá establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos.

5. La evaluación de impacto deberá incluir como mínimo:

a. Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.

b. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

c. Una evaluación de los riesgos para los derechos y libertades de los titulares a que se refiere el apartado 1.

d. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente Ley, teniendo en cuenta los derechos e intereses legítimos de los titulares y de otras personas afectadas.

6. Cuando proceda, el responsable podrá recabar la opinión de los titulares o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

7. El responsable consultará a la Agencia de Protección de Datos antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos pusiera de manifiesto que existe un alto riesgo si el responsable no toma medidas para para mitigarlo. Cuando la Agencia de Protección de Datos considere que el tratamiento previsto podría infringir la normativa vigente en materia de protección de datos, o cuando el responsable no haya identificado o mitigado suficientemente el riesgo, podrá, en un plazo de dos meses desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado. Dicho plazo podrá prorrogarse dos meses, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

CAPÍTULO VII
DISPOSICIONES APLICABLES A TRATAMIENTOS CONCRETOS

ARTÍCULO 52- Tratamientos con fines de videovigilancia

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio o bien privado.

3. Los datos serán suprimidos en el plazo máximo de dos meses desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

4. El deber de información previsto en el artículo 19 de esta Ley se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en el artículo 27 de esta Ley. El responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el artículo 19 antes citado. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

5. Al amparo del artículo 4.2.a) de la presente Ley, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. Se excluye de esta disposición el tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por parte de cuerpos de policía y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

7. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo siguiente.

8. Se prohíbe, sin excepción, el uso de sistemas de identificación biométrica en tiempo real en espacios públicos para cualquier finalidad, especialmente fines policiales o de investigación criminal.

ARTÍCULO 53- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo

1.- Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 52.4 de esta Ley.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, servicios sanitarios, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores.

ARTÍCULO 54- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

ARTÍCULO 55- Sistemas y proveedores de información crediticia

Los datos personales relativos al comportamiento crediticio contenidos en el Centro de Información Crediticia así como el funcionamiento y reglas relacionadas con los sistemas o proveedores de información crediticia se regirán por las normas que regulan el Sistema Financiero Nacional y las que al respecto dicte la Superintendencia General de Entidades Financieras (SUGEF), de modo que el acceso a dichos datos permita a las entidades financieras y de crédito valorar el nivel de riesgo de crédito de sus clientes, sin comprometer las garantías, principios y derechos concedidos en esta Ley en una medida mayor a la estrictamente necesaria para cumplir la finalidad indicada.

ARTÍCULO 56- Tratamiento de datos en la investigación en salud

1. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a. El titular o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica, en los términos previstos en la Ley 9234 Ley Reguladora de Investigación Biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b. Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c. Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. En tales casos, los responsables deberán publicar la información establecida en el artículo 19 de la presente Ley, en un lugar fácilmente accesible de la página web corporativa de la institución donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

d. Se considera lícito el uso de datos personales anonimizados con fines de investigación en salud y, en particular, biomédica. El uso de datos personales anonimizados con fines de investigación en salud pública y biomédica requerirá: a) Una separación técnica y funcional entre el equipo investigador y quienes realicen la anonimización y conserven la información que posibilite la reidentificación. b) Que los datos anonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. Sólo podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e. Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, podrán excepcionarse los derechos de los titulares previstos en los artículos 29, 30, 32 y 35 de esta Ley cuando:

i) Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados.

ii) El ejercicio de tales derechos se refiera a los resultados de la investigación.

iii) La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f. Cuando se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

i) Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 51 de esta Ley. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización de los datos.

ii) Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

iii) Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

iv) Designar un representante legal establecido en la República de Costa Rica, si el promotor de un ensayo clínico no está establecido en el territorio nacional.

g. El uso de datos personales anonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la legislación. En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe

previo del oficial de protección de datos o, en su defecto, de un experto con los conocimientos en protección de datos personales.

ARTÍCULO 57- Utilización de medios tecnológicos y datos personales en las actividades electorales

1. El tratamiento de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales deberá respetar lo indicado en el artículo 11 de la presente Ley.

2. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

3. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

4. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.

ARTÍCULO 58- Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de su número de cédula de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

2. Cuando se trate de la notificación por medio de edictos, se identificará al afectado exclusivamente mediante el número completo de su cédula de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

3. Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

ARTÍCULO 59- Derecho de rectificación en Internet

1.- Toda persona tiene derecho a la libertad de expresión en Internet.

2.- Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la

intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz.

ARTÍCULO 60- Tratamiento de datos de contacto de empresarios individuales y profesionales liberales

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 15.1.i) el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a. Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b. Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los responsables o encargados del tratamiento a los que se refiere el artículo 79 de esta Ley podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

CAPÍTULO VIII
AGENCIA DE PROTECCIÓN DE DATOS

ARTÍCULO 61- Disposiciones generales

1. La Agencia de Protección de Datos Personales, será un órgano adscrito al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt). Contará con grado de desconcentración máxima, con idoneidad especial y técnica, dotada de independencia operativa, técnica, administrativa, presupuestaria y funcional, y la potestad legalmente otorgada de dictar reglamentaciones específicas a la presente Ley, en la materia de su especialidad. Para garantizar la calidad e idoneidad de su personal, contará con los profesionales y técnicos que requiera en las materias de su competencia, incluidas personas científicas de datos y expertas en informática, ciberseguridad, entre otros, los cuales estarán sujetos a lo dispuesto por la Ley 2, Código de Trabajo, de 27 de agosto de 1943.

Su organización se definirá reglamentariamente, pero ajustará sus actuaciones a las disposiciones contenidas en esta ley.

La adquisición de bienes y servicios que realice la Agencia de Protección de Datos deberá ajustarse a la Ley 7494, Ley de Contratación Administrativa, de 2 de mayo de 1995 y su reglamento.

2. Contará con personalidad jurídica instrumental, por lo que tiene permitido celebrar todo tipo de contratos y convenios con entidades públicas o privadas, tanto a nivel nacional como internacional. Su competencia también abarca facultades plenas para conocer y resolver, ya sea por medio de denuncias o de oficio, así como sancionar, en caso de decidirlo discrecionalmente, toda conducta material o formal que configure una violación de los derechos de las personas a la protección de sus datos personales, en los términos establecidos en esta Ley y sus normas de desarrollo.

3. Sus decisiones darán por agotada la vía administrativa, sin que pudieran impugnarse las resoluciones ni ser avocadas sus competencias.

ARTÍCULO 62- Régimen económico presupuestario

1. El presupuesto de la Agencia de Protección de Datos estará constituido por:

a. Una transferencia procedente del presupuesto nacional de la República, que corresponda al menos a cinco mil trescientos nueve coma cero cinco (5 309,05) salarios base, en concordancia con la normativa dispuesta en la Ley N.° 9635, Fortalecimiento de las Finanzas Públicas, de 3 de diciembre de 2018. La Dirección elaborará el presupuesto de la Agencia de Protección de Datos y lo remitirá al jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, para su incorporación dentro del presupuesto de esta cartera ministerial, de conformidad con lo dispuesto en la Ley N.° 9524, Fortalecimiento del Control Presupuestario de los Órganos Desconcentrados del Gobierno Central, de 7 de marzo de 2018.

b. Las donaciones y las subvenciones provenientes de otros Estados, entidades públicas u organismos internacionales, que no comprometen la independencia y la transparencia de la Agencia de Protección de Datos. No se aceptarán donaciones de empresas que se dediquen a la comercialización de datos personales.

c. Los ingresos por el cobro de sanciones producto del régimen sancionador previsto en esta Ley.

2. El funcionamiento ordinario de la Agencia de Protección de Datos, así como su presupuesto, estarán sujetos a la fiscalización de la Contraloría General de la República y de la auditoría interna del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, según las competencias establecidas en la normativa vigente.

3. El o la jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones no tendrá injerencia en la asignación y ejecución del presupuesto de la Agencia de Protección de Datos Personales.

4. Se autoriza a las instituciones del Estado y entidades públicas estatales, así como a organismos nacionales e internacionales para que efectúen donaciones o aportes a la Agencia de Protección de Datos Personales y le asignen temporalmente el personal calificado para cumplir sus fines y ejecutar proyectos específicos.

ARTÍCULO 63- Funciones

La Agencia de Protección de Datos tendrá las siguientes funciones:

a. Supervisar la aplicación de esta ley y sus normas de desarrollo.

b. Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos de acuerdo con el tratamiento de los datos. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención.

c. Asesorar a la Asamblea Legislativa, al Poder Ejecutivo y otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y las libertades de las personas físicas con respecto al tratamiento.

d. Promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben.

e. Previa solicitud, facilitar información a cualquier titular, en relación con el ejercicio de sus derechos y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados.

f. Resolver las reclamaciones presentadas por un titular o un organismo, organización o asociación. Investigar el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control.

g. Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua, con el fin de garantizar la coherencia a la hora de aplicar y ejecutar las normativas en materia de protección de datos.

h. Llevar a cabo investigaciones sobre la aplicación de la normativa nacional en materia de protección de datos, en particular cuando se basa en la información recibida de otra autoridad de control u otra autoridad.

i. Efectuar un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el

desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales.

j. Fomentar el uso de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos.

k. Ser el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier convenio internacional en el que sea parte la República de Costa Rica que atribuya a una autoridad nacional de control esa competencia.

ARTÍCULO 64- Potestades

1. Para llevar a cabo las funciones de investigación, la Agencia de Protección de Datos podrá:

a. Ordenar al responsable y al encargado del tratamiento, sea organismo público o privado, que faciliten cualquier información requerida para el desempeño de sus funciones.

b. Llevar a cabo investigaciones en forma de auditorías de protección de datos.

c. Notificar al responsable o al encargado del tratamiento las presuntas infracciones en materia de protección de datos, y, transcurridos los procedimientos respectivos, aplicar las sanciones previstas en esta Ley.

d. Obtener del responsable y el encargado del tratamiento, el acceso a todos los datos personales y toda la información necesaria para el ejercicio de sus funciones.

e. Efectuar inspecciones, físicas o virtuales, a todos los locales del responsable y el encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de lo cual levantará un acta que cumpla las formalidades previstas en el artículo 270 de la Ley General de la Administración Pública.

f. Dictar las disposiciones que fijen los criterios a que responderá la actuación de la Agencia en la aplicación de la presente ley, que se denominarán circulares. Para su elaboración se deberán contar con los informes técnicos y jurídicos necesarios, y conceder audiencia a los interesados. Las circulares serán obligatorias una vez publicadas en el Diario Oficial La Gaceta.

g. Elaborar y publicar guías y manuales dirigidos a los responsables, encargados y ciudadanía en general, sobre asuntos relacionados con la protección de datos personales, para orientar a los actores hacia el cumplimiento de la legislación.

h. Acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones de la presente ley, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

Las potestades de inspección y recolección de información otorgadas a la Agencia de Protección de Datos en esta Ley, deberán ser ejercidas con sujeción a los principios de razonabilidad, proporcionalidad e interdicción de la arbitrariedad administrativa, en resguardo de los derechos involucrados, y previa comprobación de indicios suficientes que justifiquen la intervención, o la hagan necesaria para averiguar la verdad real de los hechos investigados.

ARTÍCULO 65- Dirección de la Agencia de Protección de Datos

1. La Dirección de la Agencia de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Dirección de la Agencia de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones. Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño.

3. La Dirección de la Agencia de Protección de Datos y su Adjunto serán nombrados por el Consejo de Gobierno, a propuesta del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, mediante concurso público de antecedentes entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones ordenará la publicación en el Diario Oficial La Gaceta así como en medios de comunicación colectiva, la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de las personas candidatas, el MICITT propondrá y el Consejo de Gobierno designará a la Dirección y el Adjunto de la Agencia de Protección de Datos. Una vez que el Consejo de Gobierno haya nombrado al director o directora tanto propietario como adjunto, enviará el nombramiento junto con el expediente del concurso a la Asamblea Legislativa, que dispondrá de un plazo de treinta días naturales para objetar el nombramiento por mayoría calificada. Si en ese lapso no se produjera objeción, se tendrán por ratificados. En caso contrario, el Consejo de Gobierno sustituirá a la persona cuyo nombramiento fue objetado y el nuevo nombramiento deberá seguir el mismo procedimiento previsto anteriormente.

5. El mandato de la Dirección y del Adjunto de la Agencia de Protección de Datos tiene una duración de cinco años y puede ser renovado para un único período adicional de igual duración.

La Dirección y el Adjunto solo cesarán de su cargo antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Gobierno, por:

a. Incumplimiento grave de sus obligaciones.

b. Incapacidad física o cognitiva sobrevenida para el ejercicio de su función.

c. Incompatibilidad grave por hechos sobrevenidos que impidan o dificulten que pueda ejercer las funciones atribuidas en esta Ley de forma imparcial e independiente, y en cumplimiento del interés público.

d. Condena firme por delito doloso.

La remoción de la Dirección de la Agencia de Protección de Datos por las causales de los incisos a) y c) anteriores deberá tramitarse ante el Consejo de Gobierno, mediante el procedimiento ordinario establecido en la Ley N.º 6227, Ley General de la Administración Pública, de 2 de mayo de 1978 y sus reglamentos. Una vez tramitado el procedimiento, pero de previo a la adopción de la resolución final que decida sobre la separación, el Consejo de Gobierno enviará a la Procuraduría General de la República el expediente, para que ésta se manifieste, en un plazo razonable, sobre el carácter “grave” de la falta o la incompatibilidad y la procedencia de la separación. El criterio de la Procuraduría no será vinculante pero el Consejo deberá motivar su decisión de separarse de dicho criterio, si fuera el caso.

6. Los actos y disposiciones dictados por la Dirección de la Agencia de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la jurisdicción contencioso administrativa.

CAPÍTULO IX
PROCEDIMIENTO EN CASO DE POSIBLE VULNERACIÓN A LA NORMATIVA DE PROTECCIÓN DE DATOS

ARTÍCULO 66- Régimen de reclamaciones

1. Todo titular tendrá derecho a presentar su reclamación ante la Agencia de Protección de Datos, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación aplicable en la materia.

ARTÍCULO 67- Admisión a trámite de las reclamaciones

1. Cuando se presente ante la Agencia de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a. Que no se haya causado perjuicio al afectado en el caso de las infracciones leves previstas en el artículo 76 de esta Ley.

b. Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia podrá remitir la misma al oficial de protección de datos que hubiera, en su caso, designado el responsable del tratamiento.

La Agencia podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un oficial de protección de datos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

5. La decisión sobre la admisión o inadmisión a trámite deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia de Protección de Datos.

ARTÍCULO 68- Actuaciones previas de investigación

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia de Protección de Datos podrá llevar a cabo una investigación preliminar a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

2. La investigación preliminar no podrá tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha de la resolución por la que se decida su iniciación cuando la Agencia de Protección de Datos actúe de oficio.

ARTÍCULO 69.- Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora

1. Concluidas, en su caso, las actuaciones preliminares a las que se refiere el artículo anterior, corresponderá a la Dirección de la Agencia de Protección de Datos, cuando así proceda, ordenar el inicio del procedimiento para el ejercicio de la potestad sancionadora, mediante un traslado de cargos en el que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

ARTÍCULO 70- Medidas provisionales y de garantía de los derechos

1. Durante la realización de investigación preliminar o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos.

2. En los casos en que la Agencia considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos el artículo 27 de esta Ley, la Agencia podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

ARTÍCULO 71- Sustanciación de actuaciones

En lo no expresamente previsto en esta Ley, el procedimiento administrativo se sustanciará de conformidad con las reglas para el procedimiento ordinario regulado el Libro Segundo de la Ley General de la Administración Pública.

CAPÍTULO X
RÉGIMEN SANCIONADOR

ARTÍCULO 72- Sujetos responsables

1. Están sujetos al régimen sancionador establecido en la presente ley:

a. Los responsables o corresponsables de los tratamientos.

b. Los encargados de los tratamientos.

2. No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este Capítulo.

ARTÍCULO 73- Infracciones

1. Constituyen infracciones los actos y conductas que resulten contrarias a la presente Ley. Si se ha incurrido en alguna de las infracciones tipificadas en esta Ley, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes:

a. Para las faltas leves, una multa hasta de entre diez y veinte salarios base.

b. Para las faltas graves, una multa de veinte a cincuenta salarios base, y, en caso de personas jurídicas, el monto superior entre cincuenta salarios base y hasta un dos por ciento del volumen de ventas que hubiere reportado durante el periodo fiscal inmediato anterior a la comisión de la infracción.

c. Para las faltas gravísimas, una multa de cincuenta hasta quinientos salarios base, y, en caso de personas jurídicas, el monto superior entre quinientos salarios base y hasta un cuatro por ciento del volumen de ventas que hubiere reportado durante el periodo fiscal inmediato anterior a la comisión de la infracción.

ARTÍCULO 74- Infracciones consideradas muy graves

1. Se consideran muy graves y prescribirán a los tres años las siguientes infracciones:

a. El tratamiento de datos personales vulnerando algunos o todos los principios establecidos en el artículo 13 de esta Ley.

b. El tratamiento de datos personales sin que concurra alguna de las condiciones de legitimación del tratamiento establecidas en el artículo 15 de esta Ley.

c. El incumplimiento de los requisitos exigidos para la validez del consentimiento.

d. La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e. El tratamiento de datos personales sensibles sin que concurra alguna de las circunstancias previstas en el artículo 11 de esta Ley.

f. El tratamiento de datos personales relacionados con condenas e infracciones penales fuera de los supuestos permitidos por el artículo 12 de esta Ley.

g. La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en el artículo 19 de esta Ley.

h. La vulneración del deber de confidencialidad establecido en el artículo 26 de esta Ley.

i. La exigencia del pago de un canon para facilitar al afectado la información a la que se refiere el artículo 19 de esta Ley, o por atender las solicitudes de ejercicio de derechos de los afectados previstos en el artículo 27 de esta Ley, fuera del supuestos establecido en el artículo 29 párrafo 4.

j. El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en el artículo 27 de la presente Ley.

k. La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en el artículo 45 de la presente Ley.

l. El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 64 de la presente Ley.

m. El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 44 de esta Ley cuando la misma sea exigible.

n. No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o. La resistencia u obstrucción del ejercicio de la función inspectora de la Agencia de Protección de Datos.

p. La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

q. La transferencia interinstitucional de datos personales en incumplimiento de lo establecido en el artículo 8 de la presente Ley.

r. La utilización de sistemas de identificación biométrica en tiempo real en espacios públicos.

ARTÍCULO 75- Infracciones consideradas graves

1. Se consideran graves y prescribirán a los dos años las siguientes infracciones:

a. El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela.

b. El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

c. La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.

d. La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas.

e. Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 41 de esta Ley.

f. La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

g. La infracción por un encargado del tratamiento de lo dispuesto en la presente Ley, al establecer relaciones en su propio nombre con los afectados aun cuando exista un contrato de encargo, conforme a lo dispuesto en el artículo 41 de esta Ley.

h. No disponer del registro de actividades de tratamiento establecido en el artículo 43 de la presente Ley.

i. No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 43 de la presente Ley.

j. El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 37 de esta Ley.

k. El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

l. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 25 de la presente Ley.

m. El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

n. El incumplimiento de la obligación de designar un oficial de protección de datos cuando sea exigible su nombramiento.

o. No posibilitar la efectiva participación del oficial de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

ARTÍCULO 76- Infracciones consideradas leves

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal, en particular, las siguientes:

a. El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por el artículo 19 de la presente Ley.

b. No atender las solicitudes de ejercicio de los derechos establecidos en el artículo 27 de esta Ley, salvo que resultase de aplicación lo dispuesto en el artículo 74.1.j) de esta Ley.

c. El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan tranferido los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

d. El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 5 de esta Ley.

e. La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 38 de esta Ley o la inexactitud en la determinación de las mismas.

f. No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 38 párrafo 2 de esta Ley.

g. El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

h. Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 43 de esta Ley.

i. La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales.

j. El incumplimiento de la obligación de documentar cualquier violación de seguridad.

k. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, salvo que resulte de aplicación lo previsto en el artículo 75.1 l) de esta Ley.

l. No publicar los datos de contacto del oficial de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con esta Ley.

ARTÍCULO 77- Interrupción de la prescripción de la infracción

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de doce meses por causas no imputables al presunto infractor.

ARTÍCULO 78- Sanciones y medidas correctivas

1.- Las sanciones se impondrán, en función de las circunstancias de cada caso individual, se tendrá debidamente en cuenta:

a. La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de titulares afectados y el nivel de los daños y perjuicios que hayan sufrido.

b. La intencionalidad o negligencia en la infracción.

c. El carácter continuado de la infracción.

d. La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

e. Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f. La afectación a los derechos de los menores.

g. Disponer, cuando no fuere obligatorio, de un oficial de protección de datos.

h. Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los titulares.

i. El grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado.

j. Toda infracción anterior cometida por el responsable o el encargado del tratamiento.

k. El grado de cooperación con la Agencia de Protección de Datos con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.

l. Las categorías de los datos de carácter personal afectados por la infracción.

m. La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida.

n. Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones de la presente ley, la cuantía total de la sanción no será superior a la cuantía prevista para las infracciones más graves.

4. Será objeto de publicación en el Diario Oficial La Gaceta la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la sanción resulte de una la constatación de una falta grave o gravísima y el infractor sea una persona jurídica o entidad pública.

ARTÍCULO 79- Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a. El Presidente de la República o sus vicepresidentes.

b. La Asamblea Legislativa

c. El Poder Judicial y los órganos jurisdiccionales.

d. El Tribunal Supremo de Elecciones.

e. La Administración Pública centralizada y desentralizada, excluyendo empresas públicas.

f. La Defensoría de los Habitantes.

g. Las Municipalidades.

h. Las Universidades Públicas.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refiere la presente ley, la Agencia de Protección de Datos Personales dictará resolución sancionando a las mismas con apercibimiento. La resolución ordenará asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al jerarca de la entidad responsable o encargada del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de titulares, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la Agencia de Protección de Datos propondrá también la iniciación de actuaciones disciplinarias contra los funcionarios implicados cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

4. Se deberán comunicar a la Agencia Protección de Datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán a la Defensoría de los Habitantes las resoluciones dictadas al amparo de este artículo.

ARTÍCULO 80- Prescripción de las sanciones

1. Las sanciones impuestas en aplicación de esta Ley prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la notificación al investigado, del procedimiento de investigación, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

CAPÍTULO XI
DERECHO DE INDEMNIZACIÓN

ARTÍCULO 81- Reparación del daño

1. El titular que sufra daños y perjuicios derivados de una violación de su derecho a la protección de datos personales gozará del derecho de reclamar el resarcimiento de los daños y perjuicios ocasionados en infracción de las disposiciones de la presente ley. Si dicho daño fue ocasionado por un responsable y un encargado, ambos responderán solidariamente de los daños efectivamente ocasionados.

2. El ejercicio de acciones tendientes a la reparación de los daños sufridos será ejercido en la vía judicial y operará un plazo de prescripción de un año a partir de la existencia del mismo.

ARTÍCULO 82**-** Deróguese la Ley 8968 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, del 07 de julio de 2011.

ARTÍCULO 83- Las plazas de personal, el presupuesto, bienes, equipos y todos los demás activos asignados a la Agencia de Protección de Datos de los Habitantes (PRODHAB) se trasladarán a la Agencia de Protección de Datos Personales creada en esta ley, a fin de que continúen destinados al cumplimiento de los fines de esta última.

TRANSITORIO I- El Poder Ejecutivo, en un plazo de seis meses contados a partir de la entrada en vigencia de esta ley, deberá concretar el traslado de los recursos,

bienes y personal de la Agencia de Protección de los Habitantes a la Agencia de Protección de Datos Personales, e iniciar los procedimientos para el nombramiento de los puestos de dirección de la misma, en los términos previstos por esta Ley.

TRANSITORIO II- El siguiente Presupuesto Ordinario de la República que formule el Poder Ejecutivo después de la entrada en vigencia de esta Ley, deberá reflejar el traslado de las partidas presupuestarias del programa presupuestario de la Agencia de Protección de Datos de los Habitantes hacia el título presupuestario que se creará, correspondiente a la Agencia de Protección de Datos.

TRANSITORIO III- Las personas físicas y jurídicas, públicas y privadas que ostenten condición de responsables o encargadas de datos personales gozarán de un periodo de doce meses para adecuar su funcionamiento a las disposiciones de esta Ley.

TRANSITORIO VI- La Agencia de Protección de Datos emitirá la reglamentación requerida de esta Ley en el plazo de seis meses después de su entrada en funcionamiento.

TRANSITORIO VII- La Superintendencia General de Entidades Financieras dictará las regulaciones requeridas de acuerdo al artículo 55 de esta Ley, en el plazo de seis meses a partir de la entrada en vigor de esta Ley.

Rige a partir de su publicación.

Eliecer Feinzaig Mintz

Kattia Cambronero Aguiluz

Jorge Dengo Rosabal

Diego Vargas Rodríguez

Johana Obando Bonilla

Gilberto Campos Cruz

Diputados y diputadas

17 de mayo de 2022

NOTAS: Este proyecto aún no tiene comisión asignada.

El Departamento de Servicios Parlamentarios ajustó el texto de este proyecto a los requerimientos de estructura.