ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

COMISIÓN PERMANENTE ESPECIAL DE CIENCIA Y TECNOLOGÍA Y EDUCACIÓN

LEY DE PROTECCIÓN DE DATOS PERSONALES

EXPEDIENTE N.º 23097

DICTAMEN AFIRMATIVO DE MAYORÍA

PRIMERA LEGISLATURA

DEL 1° DE MAYO DE 2022 AL 30 DE ABRIL DE 2023

AREA DE COMISIONES LEGISLATIVAS

DEPARTAMENTOS DE COMISIONES LEGISLATIVAS

DICTAMEN AFIRMATIVO DE MAYORÍA

Los suscritos diputados y diputadas, integrantes de la Comisión Permanente Especial de Ciencia y Tecnología, rendimos el presente Dictamen Afirmativo de Mayoría del expediente N°23.097, "LEY DE PROTECCIÓN DE DATOS PERSONALES", iniciativa de los diputados del Partido Liberal Progresista (PLP), publicado en el Alcance N.°102, en La Gaceta Nº 94, del 23 de mayo de 2022. Lo anterior con fundamento en las siguientes consideraciones:

1.Objeto del proyecto de ley:

La propuesta eleva la protección de datos al estándar internacional en la materia y remoza completamente el marco normativo para devolverle a las personas el control sobre su información personal. Además, el proyecto cierra portillos a los usos indebidos de datos por parte del sector público que se han dado en los últimos años. 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 El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[1], el nuevo Reglamento general de protección de datos («RGPD») regula el tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas en la Unión Europea (UE)., 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 principios 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 cincuenta 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 autorregulación. 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 entrañen 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 video vigilancia, 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.

II. Consultas institucionales:

Dicho expediente se consultó de forma obligatoria a la Corte Suprema de Justicia Y el mismo fue consultado a la Agencia de Protección de datos de los Habitantes; Agencia Protección de datos de los Habitantes; Asociación Latinoamericana Planificadores Urbanos; Caja Costarricense de Seguro Social; Cámara de Industrias de Costa Rica; Cámara de Tecnologías de Información y Comunicación; Colegio de Ingenieros Químicos de Costa Rica; Colegio de Profesionales en Informática y Computa.; Colegio de Profesionales en Sociología de C.R.; Colegio de Terapeutas; Comisión Nacional del Consumidor; Contraloría General de la República; Defensoría de los Habitantes; Fundación Privacidad y Datos; Ministerio de Ciencia y Tecnología; Ministerio de Economía, Industria y Comercio; Ministerio de Justicia; Procuraduría General de la República; Sala Tercera; Sociedad Civil Abriendo Datos Costa Rica; Superintendencia de Telecomunicaciones; Tribunal Supremo de Elecciones y UCCAEP, MIDEPLAN, Colegio de Nutricionistas, INFOCOM, Corte Suprema de Justicia.

Cumplido el plazo que establece el artículo 157, del Reglamento de la Asamblea Legislativa y, al momento de emisión del presente dictamen, se recibió la respuesta de las siguientes instituciones consultadas:

Número de oficio	Entidad	Criterio	Fecha
DFOE-GOB0364	Contraloría General de la República	De acuerdo con la iniciativa de ley consultada, se procede a indicar que el análisis a realizar por parte de este Órgano Contralor se hace en función de su ámbito de competencia, razón por la cual los asuntos de otra naturaleza contenidos en el articulado del citado proyecto que se apartan de esa premisa no son abordados considerando que por su especialidad les corresponde a otras instancias emitir opinión o criterio, conforme a las facultades que son asignadas por el ordenamiento jurídico. Partiendo de lo anterior y en términos generales, las observaciones que se hacen se presentan en cuatro temas, a saber, algunos aspectos específicos del proyecto, la nueva rectoría de la Agencia, aspectos presupuestarios y las potestades de fiscalización de la Contraloría General. **a. Algunos aspectos específicos del proyecto** El artículo 3 establece el ámbito de aplicación de la nueva ley, el mismo indica que la ley será aplicable a la administración pública centralizada y descentralizada que realizan tratamiento de datos personales en el ejercicio de sus actividades y funciones. Al respecto, aplicación de la norma debe abarcar a toda la Administración Pública en sentido amplio, es decir, no solo a la administración central y descentralizada, sino que debe ser de	12 de setiembre de 2022

		acatamiento para los órganos adscritos a estas, así como los gobiernos locales, entes públicos no estatales, empresas públicas no financieras y el sector público financiero, ello en resguardo del derecho a la intimidad de las personas regulado en los artículos 23, 24 y 28 de la Constitución Política. Otro aspecto para considerar es lo estipulado en el artículo 24 del Proyecto de Ley, en específico, lo señalado en cuanto al principio de seguridad, que en lo que interesa señala: *"ARTÍCULO 24- Principio de seguridad (...) 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 esta 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."* Siendo que la finalidad de la propuesta normativa contenida en el numeral 24 inciso 6) es el abordaje en materia de ciberseguridad, es importante señalar que actualmente existen instituciones, mecanismos y programas que tienen como finalidad el resguardo y coordinación en materia de ciberseguridad nacional, entre ellos: a) La Agencia Nacional de Gobierno Digital creada mediante la Ley NO 9943 en mayo de2021, como el órgano encargado de implementar y ejecutar servicios y proyectos transversales o estratégicos en materia de gobierno digital, incluyendo la interoperabilidad que amerita el establecimiento de medidas técnicas y legales para garantizar la seguridad de la información. Cabe indicar, que a la fecha esta Agencia aún no se encuentra operando, dado que se está a la espera de la reglamentación por parte del Poder Ejecutivo, para su posterior inicio de operaciones. b) El Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) creado mediante Decreto	

		Ejecutivo No 37052-MICIT del 9 de marzo de 2012, como un departamento del MICITT con facultades de coordinación para todo lo relacionado con la materia de seguridad informática y cibernética. c) La Comisión Nacional de Seguridad en Línea (CNSL), creada el 9 de diciembre de 2010 mediante Decreto N.º 36274-MICIT, la cual se encarga de diseñar las políticas necesarias sobre el buen uso de Internet y las Tecnologías Digitales, integrada por un representante de diferentes instituciones y organizaciones1, la cual estará presidida por el MICITT. d) El *Protocolo para el desarrollo de las acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional* (2022), el Informe 2021 Revisión de la Estrategia Nacional de Ciberseguridad de Costa Rica (2021) y la *Estrategia Nacional de Ciberseguridad de Costa Rica* (2017). Herramientas que contemplan los actores involucrados, así como sus roles y responsabilidades en las diferentes etapas de la ciberseguridad. Sobre ello, la Contraloría General ha señalado en otras ocasiones2 que la duplicidad de funciones genera mayor dificultad en la evaluación de resultados y el control de la gestión estatal. Sobre el particular, en la Memoria Anual de 2011 el Órgano Contralor propone una serie de aspectos mínimos que se recomienda al legislador considerar en las discusiones legislativas relativas al diseño institucional, entre los cuales se citan los siguientes: *¿Qué necesidad se requiere solventar de la iniciativa? ¿Cuáles son los sujetos responsables de cada una de las funciones establecidas? ¿Cuál es el esquema* *jurídico que se propone y cuál es el que mejor se adapta a los fines pretendidos por la iniciativa? ¿Existen los recursos económicos suficientes para cubrir los* *gastos futuros de la iniciativa? ¿Qué actividad alternativa se verá afectada con esta desviación de recursos y cuál será el impacto sobre la colectividad? ¿Quiénes son los operadores públicos en la actividad relacionada con esta iniciativa?* *¿Existen otras instancias con funciones similares? ¿Cuáles son los mecanismos de coordinación interinstitucional? ¿Se generan ahorros o se logran economías de* *escala con la iniciativa? ¿Se crea o se disminuye la capacidad del aparato estatal de adaptarse a nuevas realidades económicas y sociales? ¿Cuál es el grado de* *afectación sobre los recursos de libre disponibilidad del gobierno? ¿Se provoca rigidez al accionar de la política pública del gobierno? ¿Quién ejerce la política*	

		pública en esta materia? ¿Cuáles deben ser las relaciones de coordinación intra e interinstitucional para lograr los objetivos pretendidos? ¿Se establece con claridad *la obligatoriedad de tales relaciones de coordinación? ¿Ante quién rinde cuentas?* *¿Cuáles son las implicaciones del incumplimiento de las obligaciones y compromisos adquiridos? ¿Es necesario que esta iniciativa modifique o derogue el* *marco institucional existente? ¿Se consideran en la iniciativa los mecanismos de revisión institucional de frente a cambios en las motivaciones que justifican su creación?"* Aunado a lo anterior, también se encuentra en la corriente legislativa el Proyecto de Ley Número 23292 denominado "Ley de Ciberseguridad de Costa Rica", el cual busca crear un marco jurídico en ciberseguridad, en el cual se pretende crear una nueva institución pública denominada "*Agencia Nacional de Ciberseguridad*", cuya finalidad será realizar la gestión preventiva, reactiva y proactiva de las amenazas e incidentes que, a través del uso de datos, puedan generar un riesgo de seguridad para la población costarricense; y fungirá como el Centro de Operaciones de Ciberseguridad del país. Dicha Agencia se conformará por una Dirección General, un Consejo Asesor y tres unidades operativas (Centro de} Intercambio y Monitoreo de Redes (CIMR-CR), Centro de Respuesta a Incidentes de Seguridad (CSIRT-CR) y Centro de Inteligencia de Datos en Ciberseguridad (CID-CR)). En esa línea, es relevante analizar ambas propuestas legislativas, sean los Proyectos de Ley números 23097 y 23292, así como los organismos ya existentes, procurando evitar posibles problemas personales. Una máxima desconcentración del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), personalidad jurídica instrumental e independencia en su organización, funcionamiento y competencia del Poder Ejecutivo. Sobre el particular, la Contraloría General ha manifestado3 su desacuerdo respecto al otorgamiento de ese tipo de personalidad jurídica, ya que la desconcentración administrativa es una técnica suficiente en sí misma para distribuir y separar competencias dentro de una misma organización administrativa por lo que se considera que no requiere que el órgano cuente con personalidad jurídica instrumental y manejo independiente de recursos para operar y lograr sus objetivos. Asimismo, el reconocimiento de la personalidad jurídica instrumental genera que en la práctica los órganos desconcentrados operen como entidades distintas e independientes que no responden a un direccionamiento integrado por parte de sus jerarcas, lo que desnaturaliza su esencia como órganos parte de una entidad mayor, inclusive en temas de rectorías. Por lo que conviene disponer de información sobre los mecanismos de revisión	

		institucional frente a cambios en las motivaciones que justifican la creación del órgano desconcentrado, por cuanto el contexto es cambiante y puede que se requieran ajustes a la organización que se propone. De acuerdo con lo antes expuesto, se insiste en la necesidad de contar con la información necesaria para valorar la complejidad y el costo de la estructura propuesta (fines, actores, recursos, procesos y normas que integran la materia), en procura de fundamentar que corresponde a la mejor alternativa en cuanto a menor complejidad maximización de beneficios y cumplimiento de los fines propuestos; así como, otros efectos que generaría la implementación de la estructura administrativa que se pretende. En línea con lo anterior, y en lo concerniente a la calidad e idoneidad del personal, se indica en dicho numeral que los mismos estarían sujetos a lo dispuesto a la Ley N° 2 Código Trabajo. Al respecto se considera esencial aclarar el alcance de lo allí indicado, pues si bien hay artículos del Código de Trabajo que son aplicables a los funcionarios públicos, lo cierto es que los funcionarios públicos nos regimos bajo una relación estatutaria, asimismo, con la reciente promulgación de la Ley Marco de Empleo Público, No.10159, se estableció una norma específica para la mayoría del personal del sector público, con excepciones muy concretas. Debe de recordarse que la referida ley tiene como objetivo regular las relaciones estatutarias, de empleo público y de empleo mixto, entre la Administración Pública (incluido el sector público descentralizado institucional entendido este por las instituciones autónomas y sus órganos adscritos) y las personas servidoras públicas, con el imperativo constitucional de establecer un único régimen de empleo público que sea coherente, equitativo, transparente y moderno. Es en virtud de ello que debe de quedar claro el alcance en cuanto a la aplicación del Código de Trabajo a los funcionarios de la Agencia de Protección de Datos, pues se les estaría aplicando un régimen diferenciado que podría generar confusión si se trata de servidores públicos y dejando de lado la Ley Marco de Empleo Público. Adicionalmente y respecto a este mismo artículo, queda señalar que mediante el artículo 135 inciso a) de la Ley General de Contratación Pública, N° 9986 del 27 de mayo	

		del 2021, se derogará a partir del 1° de diciembre del 2022 la Ley de Contratación Pública, N° 7494 del 01 de mayo del 1996. **c. Aspectos presupuestarios** En primer lugar, es necesario iniciar con lo preceptuado en los artículos 29 y 36 del proyecto de ley donde se hace referencia a cobros de canon. En el primer numeral, específicamente, en el inciso 4), en lo que interesa, indica: "*...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."* (El resaltado es nuestro) En esa misma línea, en el artículo 36 inciso 3) señala: *"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****."* (El resaltado es nuestro) Como puede observarse en dichos artículos se encuentra regulado el cobro de un canon, pero los mismos no son mencionados como fuente de financiamiento para la Agencia y contemplados como tal, lo que denota incongruencia y evidencia la necesidad de incluir un análisis técnico que demuestre que las propuestas de las fuentes de financiamiento serán suficientes para esa nueva visión Agencia de Protección de Datos Personales que se está creando con este proyecto, máxime que no existe información en el expediente que refleje claramente las fuentes de financiamiento de la Agencia que se crea y de todas las modificaciones que se proponen, para valorar si los recursos van a ser suficientes para afrontar todos los gastos que se van a generar, tal como se indicó anteriormente. En ese sentido, de la lectura del proyecto se establece la creación de una estructura diferente a la actual para la Agencia de Protección de Datos, pues se indica que 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. Ante ello es claro que existe la propuesta de ampliar la cantidad de personal de la agencia para dar respuestas a las nuevas funciones y objetivos que se plantea para este órgano, por lo que se recalca la necesidad de realizar un	

		análisis técnico y presupuestario que pueda responder a las necesidades de esta nueva estructura. Ahora bien, en cuanto al régimen económico presupuestario para la Agencia, se encuentra regulado en el artículo 62, del cual se observan algunas incongruencias de fondo de cara a la Ley de Fortalecimiento de control presupuestario de los órganos desconcentrados del Gobierno Central, No. 9524, específicamente, en los siguientes puntos: a) El inciso 1) a) señala: *"1. El presupuesto de la Agencia de Protección de Datos estará constituido por: "Una transferencia procedente del presupuesto nacional de la República, que corresponda al menos a cinco mil trescientos nueve comas cero* *cinco (5 309,05) salarios base, en concordancia con la normativa dispuesta en la* DFOE-GOB-0364 9 20/09/2022 *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."* De la lectura de dicho inciso se entiende que los únicos recursos que se aprobarían desde el presupuesto de la República son los correspondientes a dicha transferencia, sin embargo, conforme a la Ley No. 9524, específicamente, en su artículo 15, estipula que todos los presupuestos de los órganos desconcentrados de la Administración Central serán incorporados al presupuesto nacional, nótese que no se hace ningún tipo de diferenciación, por lo que la Agencia debe de presentar todo su presupuesto, para que este sea integrado y aprobado según las reglas del Presupuesto de la República y bajo los principios de universalidad y unidad presupuestaria. Es importante recalcar que el objetivo de la norma supra citada es que todo presupuesto de un órgano desconcentrado debe estar incorporado en el presupuesto nacional, sin que se haga diferencia entre los ingresos del órgano según su origen, por lo que no se debería de incorporar en forma separada del resto de los ingresos del presupuesto nacional. Cabe advertir, que una separación de los ingresos dejaría sin efecto el artículo 8 de la Ley de Administración Financiera de la República y Presupuestos Públicos. (En esta misma línea, obsérvese lo indicado en el DictamenC-072-2019 del 10 de marzo de 2019)6 b) Finalmente, el inciso 3)7 señala que el jerarca del MICITT no tendrá injerencia en la asignación y ejecución del presupuesto de la Agencia, lo que lo hace contrario a lo	

		estipulado en la Ley No. 9524 y su reglamento. Esto por cuanto en dichas normas se establecen facultades al ministro para que éste asigne recursos si el anteproyecto no es presentado en el plazo estipulado. Además, le concede las potestades para el seguimiento y evaluación presupuestarias, lo cual debe de realizarse en forma integral con el presupuesto del Ministerio (al respecto, obsérvese lo estipulado en los artículos 8 y 15 del Reglamento a la Ley N° 9524 Ley de Fortalecimiento del control Presupuestario de los Órganos Desconcentrados del Gobierno Central Nº 42712-H). Asimismo, el jerarca de cada Ministerio tiene la potestad de pronunciarse respecto a las modificaciones presupuestarias, plazos y requerimientos adicionales, ello conforme lo señalado en el artículo 11 del Reglamento supra citado. Debido a esto es claro que estas potestades dadas al jerarca tienen como fin lograr una coordinación y orientación general del Ministerio rector, acción que no es contraria a la independencia con la que deban ejercer sus funciones los órganos con desconcentración máxima. (Para mayor abundamiento, obsérvese lo señalado en el Dictamen C-073-2022 de fecha 05 de abril de 2022.) **d. Potestades de fiscalización** El artículo 8 del proyecto de ley regula el tratamiento de datos por obligación legal, interés público o ejercicios de poderes públicos y transferencia interinstitucionales. Dicho artículo, en su inciso 3, indica -en lo que interesa- lo siguiente: *"…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: …/ … **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**.”* (El resaltado es nuestro) Al respecto, es necesario tener presente las potestades de fiscalización que posee este órgano contralor para el ejercicio de sus funciones, las cuales se encuentran reguladas en diferentes leyes que le facultan para tener acceso a cualquier fuente o sistema de} información, registro, documento, instrumento, cuenta o declaración, a la contabilidad, correspondencia para el ejercicio del control y fiscalización de la Hacienda pública tal y cómo está estipulado en el artículo 13 de la Ley Orgánica de la Contraloría. En igual sentido, se tiene que el artículo 11 de la Ley contra la Corrupción y el enriquecimiento ilícito en la función pública, No. 8422, regula el acceso a la información otorgando a la Contraloría una serie de potestades para el ejercicio de sus funciones en aras del resguardo de la Hacienda pública. Aunado a las normas anteriores, se tiene también normativa expresa la cual señala un velo de confidencialidad durante las investigaciones que realiza este órgano constitucional, como lo es la Ley General de Control Interno, No. 8292, la cual en su artículo 6 estipula la obligación de guardar la confidencialidad de la información, documentación y otras evidencias de las investigaciones que efectúan las auditorías internas, la administración y la Contraloría hasta la formulación del informe respectivo. En ese mismo sentido, véase el artículo 8 de la Ley contra la Corrupción y el Enriquecimiento Ilícito en la función pública, No.8422. De conformidad con las normas señaladas no cabe duda la competencia otorgada a la Contraloría General para ejercer	

		su potestad de fiscalización, por lo que resulta esencial hay que señalar que lo dispuesto en el artículo 8 del proyecto de ley no afectaría las competencias de investigación dadas a esta Contraloría General y que se respetaría el velo de confidencialidad durante la etapa de investigación. Es por ello que es relevante que se valore como una de las excepciones del artículo 8 del proyecto, esta potestad, a efectos de que cuando se esté en el ejercicio de las funciones de fiscalización sean estas investigaciones o auditorías donde se está trabajando con transferencia de datos personales este órgano contralor sea considerado como una de las excepciones citadas en el artículo. El artículo 33 regula sobre el derecho a no ser objeto de decisiones individuales automatizadas, el cual en lo que interesa reza: *"…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..."* Sobre ello es necesario recordar la potestad que ostenta esta Contraloría General estipulada en el artículo 23 de la Ley contra la Corrupción y el enriquecimiento ilícito en la función pública, No. 8422, donde podrá exigir por medio de una orden singular que el servidor público que no esté obligado a presentar la declaración jurada deba presentar para realizar averiguaciones y los estudios pertinentes para determinar un eventual enriquecimiento ilícito o cualquier otra infracción a la presente ley, por lo que se ve necesario que dicho artículo 33 contemple como una excepción la declaración jurada regulada en los artículos 21 y 23 de la Ley No. 8422.	
CPSCR-JDR-043	Colegio de Profesionales en Sociología	Indican que no le es posible dar un criterio sobre este expediente	17 de agosto del 2022
CPIC-JD-13-2022	Colegio de Profesionales en Informática	Esta asesoría concluye que, en definitiva, la protección de datos personales requiere de una norma que sea conforme a los tiempos actuales y futuros. Desde ese punto de vista, el interés de los diputados proponentes por crear esa ley es de relevancia para el país. No obstante, a partir de las observaciones hechas al texto propuesto mediante este criterio, concluimos que el proyecto de ley adolece de	22 de agosto del 2022

		problemas de técnica legislativa y redacción, que haría difícil a los responsables y a los operadores jurídicos su aplicación, pero, también dificultaría la comprensión de esta ley por parte del ciudadano común. Dado que la materia es compleja, pero de absoluta relevancia, la recomendación es comunicar a la Comisión de Asuntos Económicos, que, si bien el Colegio apoya la aprobación de una ley de protección de datos en el sentido propuesto, no está de acuerdo con la aprobación este texto del proyecto de ley en la forma en la que se encuentra redactado actualmente. Que, en ese sentido, el Colegio recomienda la elaboración de un texto sustitutivo donde se consideren las observaciones hechas a la propuesta, se ordene y simplifique la redacción del articulado y se eliminen aquellos artículos que puedan implicar la violación	
No detalla número de oficio	Asociación Latinoamericana de Internet	Esta asesoría concluye que, en definitiva, la protección de datos personales requiere de una norma que sea conforme a los tiempos actuales y futuros. Desde ese punto de vista, el interés de los diputados proponentes por crear esa ley es de relevancia para el país. No obstante, a partir de las observaciones hechas al texto propuesto mediante este criterio, concluimos que el proyecto de ley adolece de problemas de técnica legislativa y redacción, que haría difícil a los responsables y a los operadores jurídicos su aplicación, pero, también dificultaría la comprensión de esta ley por parte del ciudadano común. Dado que la materia es compleja, pero de absoluta relevancia, la recomendación es comunicar a la Comisión de Asuntos Económicos, que, si bien el Colegio apoya la aprobación de una ley de protección de datos en el sentido propuesto, no está de acuerdo con la aprobación este texto del proyecto de ley en la forma en la que se encuentra redactado actualmente. Que, en ese sentido, el Colegio recomienda la elaboración de un texto sustitutivo donde se consideren las observaciones hechas a la propuesta, se ordene y simplifique la redacción del articulado y se eliminen aquellos artículos que puedan implicar la violación Sugieren aprobar con dispensa de trámites en Comisión	29 de julio de 2022
JD-0184-08-2022	Colegio de Farmacéuticos	Debemos indicar en primer término que desde el Colegio de Farmacéuticos de Costa Rica vemos de muy buena menara que se busque fortalecer el régimen de protección de los datos personales de los habitantes, a partir de una reforma legislativa que busque poner a tono nuestro marco jurídico con las mejores prácticas en este campo que podemos traer desde el Derecho Comparado. En resumen, en este proyecto de ley hemos identificado: 1.- Se amplía el diccionario de definiciones. 2.- Se amplía el ámbito de aplicación 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.	03 de agosto de 2022

		3.- Regula el procedimiento de los datos de las personas fallecidas y de las personas vinculadas al fallecido. 4.- 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. 5.- 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, JD-0184-08-2022 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. 6.- 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. 7.- En cuanto a las sanciones, se incrementa su cuantía económica. 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. 8.- Se 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. 9.- Las sanciones se tipifican en faltas leves, graves y gravísimas, según la infracción realizada. 10.- Para las faltas leves, una multa hasta de entre diez y veinte salarios base. 11.- 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. 12.- 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. Reiteramos que es importante que Costa Rica se sume a las mejoras prácticas en materia del debido resguardo y protección de datos personales, siendo que esta reforma se inspira en 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. Tal y como se indica en la exposición de motivos de la iniciativa de ley, Costa Rica ha manifestado su intención de adherirse al Convenio 108, siendo este el único tratado internacional de alcance global existente hoy en materia de Protección de Datos Personales. En lo que se refiere propiamente al INS revisado el proyecto, no hay objeciones, ni observaciones de fondo y forma, y no se encuentran elementos lesivos para la Institución. Esa adhesión implicaría que nuestra legislación se adecúe no solo al Convenio, sino también a su Protocolo, que se conoce como "108" en armonía con el RGPDP; lo que sin duda brindaría mayor seguridad jurídica, como un factor crítico de atracción para la inversión digital, donde se valora altamente la existencia de un entorno jurídico seguro para la protección de datos. Nos parece importante que se mantenga una particular referencia de los datos personales sensibles y que se tenga expresa mención del dato en salud, expuesto en el acápite de definiciones, donde se indica: i *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;* Consideramos, que si, aunque pudiese derivarse de su redacción, no está de más señalar: *incluida la prestación sanitaria en el ámbito público y privado.* En cuanto al artículo 10, referente al tratamiento de los datos personales sensibles, se excluye de ese tratamiento a los datos relativos a la salud, salvo: *(…)* *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.* En el inciso f) si bien más adelante se hace puntual mención en el CAPÍTULO VII DISPOSICIONES APLICABLES A TRATAMIENTOS CONCRETOS, al Tratamiento de datos en la investigación en salud (artículo 56), incluiríamos investigación en salud. En cuanto al inciso g), con la experiencia de la pandemia que ha enfrentado el mundo, consideramos que debe incluirse en ese artículo los supuestos de pandemias debidamente declaradas. En cuanto a ese numeral, *in fine*, ya existe una obligatoriedad de secreto profesional a nivel deontológico y toda legislación referente al secreto profesional que en futuro se fuese a dictar, debe ser consultada a los colegios profesionales. Sobre el mencionado CAPÍTULO VII DISPOSICIONES APLICABLES A TRATAMIENTOS CONCRETOS; consideramos que en virtud de los particulares alcances de la relación clínica, debe valorarse el dictado de algunas disposiciones generales en orden a esta relación. Finalmente, estimamos importante la naturaleza jurídica que se le brinda a la PROHAB, como órgano con máxima desconcentración, personería jurídica instrumental y su propio presupuesto y si llamamos la atención en orden a los montos fijados para las multas, toda vez que, en el caso, por ejemplo de las multas por faltas se dispone: *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. Nos preocupa el hecho no solo de los elevados montos, que, si bien son un factor de disuasión frente al infractor de la ley, representan sumas muy cuantiosas que tratándose por ejemplo de los colegios profesionales (que son personas jurídicas) tienen una realidad económica que dista por mucho de empresas de ventas, siendo que la ley incorpora ese concepto al hablar de volumen de ventas. O bien deben revisarse los montos o bien debe establecerse una diferenciación, pues no todas las personas jurídicas son empresas de ventas no tienen el mismo componente presupuestario	
DE-086-22	UCCAEP	La UCCAEP considera que es necesaria una reforma integral a la Ley N° 8968, en virtud de que la tutela a la intimidad implica, la posibilidad real y efectiva para el ciudadano de saber cuáles datos suyos están siendo tratados, con qué fines, por cuáles personas y bajo qué circunstancias, esto para que pueda ejercer el control correspondiente sobre la información que se distribuye y que lo afecta. No obstante, se solicita se incorporen algunas observaciones de fondo, con el fin de que la futura norma integre los principios y mejores prácticas internacionales en materia de protección de datos. De la misma forma, nos ponemos a disposición de la Comisión de Ciencia, Tecnología y Educación, con el fin de realizar una presentación para abordar los cambios en el texto legislativo, propuestos por UCCAEP .	30 de agosto del 2022
No. SP155-2022	Corte Suprema de Justicia	Con base en las consideraciones expuestas, determina que el proyecto de Ley sometido a consideración sí afecta la organización y funcionamiento del Poder Judicial, toda vez que se requiere reorientar la asignación de recursos humanos, financieros, tecnológicos y otros, para la adecuada gestión de las distintas bases de datos que se manejan a lo interno del Poder Judicial. A su vez, podrían requerirse eventuales modificaciones en la estructura organizativa de las dependencias técnicas internas, que habrían de asumir las distintas funciones y deberes previstos en la Ley. Finalmente, considero que, tanto la implementación material de la Ley, como la reorganización funcional surgida como consecuencia directa de aquella, conlleva un indudable impacto financiero y presupuestario que deberá ser valorado en función del aspecto cuantitativo y cualitativo de los ajustes que sean requeridos de aprobarse la misma; lo que implica hacer las previsiones presupuestarias correspondientes	19 de agosto del 2022
MJP-DM-837-2022	Ministerio de Justicia y Paz	PRIMERO: Coincidimos con la exposición de motivos del proyecto, sobre la necesidad de generar un marco normativo nuevo de protección de datos personales acorde a las necesidades actuales; sin embargo, deben realizarse las siguientes consideraciones generales: a. En la propuesta se valora la experiencia adquirida con la	07 de setiembre del 2022

		implementación de la Ley N°8968 Protección de la Persona frente al Tratamiento de sus Datos Personales, y los más de diez años de vigencia; y se realiza una exposición de los retos actuales como país y los vacíos de la ley vigente, no obstante, como se expondrá más adelante no solventa algunos de los problemas de la actual normativa y debe darse un impulso realista desde la promulgación para que no se repita el proceso anterior. b. El proyecto muestra cambios sustanciales dirigidos a adecuar la legislación nacional con los estándares establecidos por la Unión Europea y en los Estándares emitidos por la Red Iberoamericana de Protección de Datos Personales, lo cual viene iniciar el proceso para la adhesión al Convenio 108, 108 y sus protocolos, lo cual se ha venido postergando; esto también se evidencia al promover el flujo transfronterizo de datos personales y establecer reglas claras para promover una economía digital y convertir a nuestro país en una zona segura de transferencia, lo nos generaría una ventaja competitiva en la Región. Este proyecto también permitiría contar con una legislación más robusta para promover el cumplimiento en el sector público de la normativa de protección de datos personales y evitar casos que violenten los derechos de los ciudadanos en este materia y detener malas prácticas que van desde dar tratamiento a datos personales sin contar con las condiciones mínimas, dar acceso sin justificación alguna a bases de datos o de asignar los recursos necesarios para la atención de los riesgos evidenciados . c. El traslado del ministerio al que esté adscrita la Agencia, es un tema de relevancia dado que la condición de autonomía plena, que actualmente se reprocha, con o sin fundamento, no se resuelve e incluso al trasladarla a una estructura de tamaño menor, viene a limitar el crecimiento futuro por el llamado “techo presupuestario”; por lo que resulta de mayor relevancia que se dote de la autoridad regulatoria necesaria, así como de las herramientas para la investigación, supervisión y ejecución de proyectos en materia de protección de datos personales y con esto un presupuesto suficiente que permita contar con la estructura organizacional y el personal requerido para el cumplimiento de todas las atribuciones que le conceden a la Agencia; esto como parte de las lecciones aprendidas con la norma actual, ya que en su momento el país contó con una normativa destacada a nivel regional pero que con el paso del tiempo no se dotó a la Agencia de las condiciones requeridas para su difusión e implementación y con esto generar el cambio en todos los sectores respecto al tratamiento de datos personales. Un punto que debe resaltarse es la forma de designación de quien ejerza la Dirección de la Agencia y que su nombramiento será por un plazo determinado, lo que permite planificar y establecer proyectos a mediano plazo. No obstante, se omite indicar respecto a prohibiciones posteriores al ejercicio del cargo,	

		lo cual es necesario. El argumento de que es “más razonable” la ubicación en el MICITT, puede ser contraproducente también técnicamente, ya que se desconoce, por completo dentro del proyecto, el tratamiento de datos personales por medio manuales, lo cual es un riesgo para el cumplimiento de la normativa; un ejemplo de ese tratamiento son todos los expedientes de personal, los expedientes de procedimientos sancionatorios, inscripciones o solicitudes que aún se realizan en físico. d. Es recomendable hacer una revisión completa de la redacción del texto para darle mayor claridad, siendo que tiende a generar confusiones y esto es una limitante de la legislación actual, tanto la Ley N° 8968 como del reglamento, ya que son confusas y hasta contradictorias, por lo que si se pretende una legislación robusta y de oportuna aplicación, debe de ser clara, para que la Agencia pueda ejecutar las atribuciones establecidas y también para que el habitante le resulte comprensible los derechos y las protección a los mismos. En este punto la revisión del texto es importante dado que en muchos artículos se hace remisión a otros del mismo cuerpo normativo o de otro, lo que genera situaciones como las que presentan los artículos 57.1 y 74 apartados e) y f) donde el texto no coincide con el numeral que referencian; o situaciones como en el artículo 61 que se refiere a una Ley que ya ha sido reformada en su totalidad y estamos a pocos meses de que entre a regir una nueva ley. Este estudio es importante también que se realice desde la óptica de especialistas en derecho administrativo, ya que el texto de propuesto es muy técnico, desde la óptica de protección de datos personales(lo cual cumple plenamente), pero hay cuestiones que no son de esa materia sino de derecho administrativo e incluso de derecho administrativo sancionatorio, por lo que no son abordadas en algunos artículos de la mejor forma, por ejemplo, en los temas de prescripción, ya que es confuso las regulaciones de interrupción, reinicio del conteo, plazos para aplicación del conteo e incluso se deja de lado o se confunde con la caducidad del procedimiento. e. Por otro lado, dentro del texto es común que se indique protección de datos sin que se incluye la palabra personales, siendo un aspecto importante para delimitar la materia a la cual se refiere; este detalle debe corregirse incluso en el nombre de la autoridad, ya que en gran parte del texto no se incluye su nombre completo lo que puede inducir a error, sobre la materia en la cual tiene competencia. f. Cuando se refiere a las medidas técnicas físicas y lógicas, es importante mencionar las administrativas, porque son los lineamientos, políticas, normativas y afines que propician/soportan/respaldan la aplicación de las medidas técnicas, físicas o lógicas. g. Dentro del proyecto se establecen diferentes terminologías para referirse a los	

		entes que integran el sector público, utilizando conceptos que dejan en algunos artículos por fuera a cierto tipo de entes; esto debería estandarizarse a sector público sin hacer distingos, ya que en la práctica puede prestarse a confusión y a que queden ciertos grupos a conveniencia para cumplir o no lo que se pretende regular. h. El tema de la comercialización de datos personales se excluye en su totalidad y es una actividad que debe incluirse, debido a las repercusiones que tiene, ya que esta actividad no solo se presenta en operaciones asociadas con instituciones reguladas por SUGEF, sino en no reguladas; además de actividades conexas a estas como las labores de cobro, donde debe protegerse el derecho del habitante, pero también de quien legítimamente puede ejercer acciones cobratorias. Si bien se considera de forma positiva que no se deba "inscribir" ante la Agencia las bases de datos de quienes comercialicen los datos personales, si es necesario regular de forma efectiva esta actividad y que incluso deba realizarse una "notificación" a la Agencia sobre la existencia de una base de datos junto con registro de actividades de tratamiento, cuando se comercialicen datos personales o se ejerzan cierto tipo de actividades que puede establecer la misma Ley. i. Debe clarificarse si a las instituciones del sector público, también se le impondrán sanciones económicas. SEGUNDO: En lo que respecta al Capítulo 1 de disposiciones Generales, podemos acotar que: a. En cuanto al objeto debe indicarse expresamente que su aplicación refiere tanto al tratamiento de datos personales realizado por cualquier medio, ya sea manual o automatizado. En este artículo si debe de recalcarse lo indicado respecto a la redacción y terminología utilizada, ya que se utiliza vocablos que no colaboran en la definición del objeto de la norma, tal como "elevar el nivel de protección" o "facilitar el flujo", donde debería establecerse acciones como "garantizar", "regular" y siendo también necesario simplificar la redacción ya que se incluyen argumentaciones o justificaciones del objeto, más no la definición del objeto propiamente. b. En las definiciones consideramos importante rescatar nuevamente lo indicado respecto a la revisión de la redacción, para que sea clara y comprensible, adicionalmente: i. En la definición de base de datos debe aclararse su definición, que incluir "manual o automatizado" y "con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización". Esto toma importancia, porque aún muchas instituciones y empresas (incluso pensando en pequeñas empresas) no tienen sistemas digitalizados de información o incluso en casos particulares, aunque se tenga en digital debe recurrirse a tratamiento de datos en físico (ejemplo situación reciente de la CCSS y EDUS) ii. Se utilizan términos que no son usuales en nuestro medio; tal como "revelación de datos" siendo más claro "comunicación de datos", por citar un ejemplo. iii. Se debe clarificar la definición de fuentes de	

		acceso público, eliminando incluso los ejemplos que se indican en la misma. Y si se refiere a bases de datos de acceso público, debe depurarse el concepto, dado que los ejemplos que cita incluso a la fecha, no todos tienen norma expresa habilitante. IV. Debe incluirse los términos: tipos de datos personales (no solo sensibles) y por ende el desarrollo de las condiciones particulares de cada tipo, comercialización de datos personales, información por capas, doble capa informativa, política transparente de datos personales, mercadotecnia directa. c. El articulo 9 propuesto, debe revisarse su redacción bajo lo establecido en la Ley No. 10238 de reciente aprobación; al igual que otros numerales que refieren a personas menores de edad. TERCERO: En lo referente al capítulo II, consideramos importante indicar: a. La incorporación taxativa de los principios es relevante y contemplar la evolución de estos; pero debe incorporarse que el análisis de los mismos siempre se realizará en favor del habitante y ante cualquier imprecisión su interpretación deberá realizar en favor de este. b. En referencia al artículo 16, en el punto 6. debe indicarse que debe darse la posibilidad al usuario para que este marque afirmativa o negativamente, y que no esté previamente seleccionado. c. En el numeral 18, debe clarificarse la redacción, e indicarse en términos generales que son desleales los tratamientos de datos personales cuando se genere una exclusión no fundamentada. d. En lo referente al principio de transparencia desarrollado en el artículo 19, dentro de la información que debe proporcionarse al titular debe estar los datos de identificación, ubicación y todos los datos de contacto del destinatario de una transferencia de datos personales, así como las condiciones y fundamentación en que se realizó en transferencia; esto con el fin de que el titular pueda ejercer ágilmente sus derechos y no como una discrecionalidad del responsable del tratamiento. e. En el numeral 20.3 debe indicarse expresamente que no se considera incompatible con las finalidades iniciales si los datos se trasladan sin que se pueda identificar algún titular. f. En el numeral 22.2 debe incluirse expresamente todos los respaldos que tenga de los archivos, registros, bases de datos, expedientes o sistemas de información. g. En el numeral 23.4, debe agregarse un plazo máximo para realizar esas revisiones y evaluaciones; ya que si bien se indica que permanentemente estas acciones deben estar debidamente documentadas y que al menos una vez año las debe realizar de forma integral si se trata de datos sensibles. De la misma forma en el 23.3.d, debe indicarse la periodicidad máxima o establecerse que en el reglamento se establecerá de acuerdo al nivel de riesgo. h. No se considera atribución atinente a las competencias de la Agencia el establecer “un estándar mínimo de ciberseguridad para el sector público”, como lo indica el artículo 25.6., ya que esto compete a otras instancias. i. En	

		el artículo 26 debe indicarse claramente que la confidencialidad aplica respecto a los datos personales y su tratamiento, más no sobre irregularidades que se presenten en el mismo. CUARTO: En lo que respecta al capítulo III de derechos del titular, debemos indicar que: a. El articulo 28.6 debe indicarse claramente que serán gratuitas para el titular, el tutor o representante legal del titular las solicitudes de ejercicio de los derechos, ya que la redacción propuesta es ambigua. b. En el numeral 29.1.c se indica "categorías de destinarios" no obstante no se define o establece a que se refiere ese concepto o que tipos existen. E igualmente consideramos necesario que se indique los datos de identificación, contacto y comunicación de a quien se transfirió para que pueda ejercerse los derechos plenamente; igualmente en el artículo 29.1.f es necesaria la identificación y datos de contacto de quien obtuvo los datos personales para que el habitante conozca a quien dirigirse para el ejercicio de sus derechos; así como la información del acto de transferencia. En lo que se indica al cobro de un "canon razonable" (artículo 29.4 y 36.3) no se considera adecuado el cobro de "solicitudes reiteradas", debido a lo dificultad para definir el concepto, ya que en muchos casos los titulares deben solicitar el acceso, luego la rectificación o cancelación de datos y nuevamente requieren realizar el acceso de información ya que el responsable no ejecutó lo solicitado y es el mecanismo para presentarlo de prueba en el procedimiento de protección de derechos; (es común ese requerimiento por parte de los titulares) por lo que ese costo puede limitar el ejercicio de los derechos. En el 29.4, a efectos de la portabilidad debe indicar que debe ser un formato abierto, neutral e interoperable. La entrega de la información debe tener plazos de entrega establecidos. d. En el artículo 31, consideramos oportuno que debe establecerse una regulación de plazos máximos para la aplicación del derecho al olvido, donde se evidencie la proporcionalidad; ya que al ser limitaciones no deberían reservarse para el reglamento Este plazo debe contemplar otros marcos normativos, como por ejemplo los plazos para la cancelación de asientos en el Registro Judicial de las personas sentenciadas luego del cumplimiento de la pena; ya que cuestiones administrativas se les asigna antojadizamente plazos superiores a una cancelación de un asiento de condena judicial, siendo esto de un impacto mayor de incumplimiento del marco normativo; por lo que si debe establecerse plazos de referencia para la aplicación de derecho al olvido. Consideramos necesario se agregue a ese numeral que el responsable deberá notificar al titular de la cancelación, indicando los datos cancelados y las implicaciones de la acción realizada. e. En el artículo 33, donde se refiere al derecho de obtener una "intervención humana significativa"; consideramos que debe indicarse	

		que el interesado se le dará audiencia por la cantidad de días que se establezca para que aporte los argumentos y documentación que considere relevante; y también indicarse al final que debe notificársele el resultado final de esta diligencia. f. Respecto a lo que indica el numeral 34.2, cuando se transfieran datos entre responsables, debe obligatoriamente notificarse al titular, ya que a partir de ese momento se generan nuevas responsabilidades hacia el titular. En cuando al numeral 34.3, no se entiende si no afectará los derechos y libertades de otros titulares, de otros derechos o de otros que no se determina con claridad. g. En lo que respecta a la limitación del tratamiento de datos personales (artículo 35) debe mediar una comunicación expresa entre las partes. h. En el artículo 36.1 debe indicarse que no solo debe establecer el medio y el procedimiento, sino darle publicidad y que sea de acceso fácil al habitante. QUINTO: Respecto al capítulo IV del responsable y encargado del tratamiento a. En el artículo 37.1 y 40.2 cuando se menciona “y sus normas en desarrollo” este término debe modificarse por un término de uso generalizado, tal como “y normas conexas”, si es ese el sentido de la expresión. En el numeral 37.2.e, consideramos oportuno agregar expresamente migrantes, ya que se requiere visibilizar esta situación. b. En el numeral 39.2, debe incluirse expresamente la comunicación de datos entre el OIJ, entre los diferentes cuerpos de policía establecidos en la Ley General de Policía, incluso policías municipales y con cuerpos de policía internacionales, que se fundamente en una investigación; siempre mediando el establecimiento de los protocolos y medidas de seguridad necesarios. En el artículo 39.2.d debe indicarse que es aplicable en el tanto se recurra a mecanismos de anonimización. Asimismo, en el artículo 39.5, debe indicarse que se obliga a las disposiciones de esta Ley, así como a las disposiciones especiales establecidas por el transmitente o por el titular. c. En el artículo 43, en cuanto al registro de actividades de tratamiento se establece el contenido mínimo, pero debe introducirse la obligatoriedad de contar obligatoriamente con la documentación que respalda el contenido del registro. En el numeral 43. d, como se ha reiterado debe incluirse los datos de contacto. En lo que respecta a lo formulado en el artículo 43.5, no estamos de acuerdo con la disposición de que no sea obligatorio para las empresas u organizaciones con menos de 50 personas, debido a que esto genera un portillo para cierto tipo de actividades (ejemplo la de cobranzas) para que establezcan diferentes patronos con menos de 50 personas cada una, con el fin de evadir obligaciones; por lo que debe eliminarse esa opción en solitario y que se lea “ menos de 50 personas y se encuentre registrada y al día	

		como PYME" d. En el numeral 44.2 se indica que "solo por el plazo de prescripción de estas", no obstante, debe indicarse a cuál plazo de prescripción se refiere, ya que pueden existir diferentes tipos de responsabilidades con diferentes plazos de prescripción, por lo que no estaría claro cuándo podría procederse con la "destrucción de los datos" SEXTO: En cuanto a lo que propone para las transferencias internacionales en el capítulo V, podemos indicar: a. En el artículo 45.1 debe aclararse si se refiere al nivel de protección de los datos de las personas físicas o si en realidad se refiere al nivel de protección de las personas físicas propiamente. b. En el numeral 45.d, se refiere a que el exportador ofrezca garantías suficientes y acredite el cumplimiento de las condiciones mínimas y suficientes aplicables a la materia, no obstante, no es claro la aplicación del término suficiente ni a quien o quienes debe acreditarle el cumplimiento. Adicionalmente consideramos importante indicar que normas y condiciones aplicarían para cuando se dé la importación de datos personales. Otro punto que se ha prestado a discusión con la actual ley es lo referente a intermediarios tecnológicos y no hay una referencia normativa al respecto dentro del proyecto. SETIMO: Respecto al capítulo VI, referente a medidas proactivas, debemos indicar: a. Que consideramos relevante la incorporación de este tipo de medidas debido al impacto que tienen el tratamiento de los datos personas. Cabe indicar que debe valorarse el impacto de estas medidas en el sector público, ya que genera cambios en procedimientos, incorporación de plazas con especialidades que en este momento no existen y que requieren un estudio de cargo en cada institución; además de que debe tomarse en cuenta si se va establecer unidades aparte para que asuman esas funciones también requiere un estudio técnico específico. Este punto es relevante por las previsiones presupuestarias que debe realizarse para cumplir con la normativa y los plazos de los transitorios. b. En el numeral 48 debe incorporarse, en la lista de quienes están obligados a designar un Oficial de Protección de Datos personales, a las escuelas y colegios, a la Asamblea Legislativa; además de que debe clarificarse respecto a las entidades financieras sin supervisión de SUGEF y también a empresas que tenga un número considerable de empleados. En el aparte 3 dentro de la información que debe remitirse sobre el cese de un Oficial de Protección de Datos Personales debe incluirse el motivo. Y en el aparte 4 consideramos necesario que, en el caso del Sector Público, cada institución debe tener un Oficial de Protección de Datos Personales a tiempo completo, ya que si no sería un recargo de funciones con los efectos usuales de incumplimiento en el ejercicio de alguna de las funciones encomendadas.	

		Debe incluirse prohibiciones específicas para el cargo de Oficial de Protección de Datos Personales (durante y posterior al nombramiento), así mismo la obligación de confidencialidad establecida en el aparte 8, debe revisarse su redacción. En cuanto al Oficial de Protección de Datos Personales, debe esclarecer si es uno por institución o empresa o por base de datos, ya que la redacción tiende a confundir respecto a este punto. Y en lo público debe clarificarse, con el fin de que se establezca quien realiza la selección final de este funcionario(s) y el tipo de nombramiento. El establecimiento del perfil general de las personas físicas o jurídicas, para ejercer ese cargo, debe realizarse vía reglamentaria, ya que no existe certeza de que se cuente con la cantidad de personas formadas para la implementación completa de todos los puestos requeridos, en el sector privado y en lo público; incluso puede pensarse en un mecanismo de certificación y registro de los mismos por parte de la Agencia. Este punto es importante, ya que en el caso del Sector Público este tipo de clasificaciones y especialidades aún no han sido establecidas, y debe generarse la creación de ese tipo de plazas, pero también con un perfil determinado, no simplemente asignar un puesto, ya que la responsabilidad es un componente asociado la clasificación de los puestos. El transitorio de implementación de esta figura debe contemplar que debe realizarse todo el proceso dentro del régimen de empleo público. c. En lo referente a las evaluaciones de impacto, establecidas en el numeral 51, debe clarificarse si puede contratarse la realización de la evaluación o si únicamente puede realizarla el responsable. OCTAVO: Respecto al capítulo VII, sobre disposiciones aplicables a tratamientos concretos, consideramos que: a. Debe ampliarse el concepto de video vigilancia, ya que únicamente se refiere a cámaras fijas y deja de lado cámaras móviles, incluso dispositivos tales como drones donde también pueden ser utilizados con fines más allá de la seguridad de personas y bienes. b. Respecto a los sistemas y proveedores de información crediticia, consideramos que en el proyecto se desconoce lo referente a la comercialización de datos personales y esta actividad no solo se realiza por entes relacionados a el Sistema Bancario Nacional y que se encuentren regulados; además de que la regulación que se ejerce sobre estos no refiere al uso de datos personales y a la comercialización de los mismos, por lo que abre un portillo preocupante para esta Agencia, dada la incidencia de esta temática en las denuncias que se presentan, por lo que el habitante no tendría como hacer valer sus derechos. c. En el artículo 56,	

		en el aparte a. que debe consignarse una redacción que englobe la normativa vigente y futura de esta materia y no limitarlo a la Ley No. 9234. En el apartado b. debe realizarse la misma observación realizada en otros numerales de que “sin que permita la identificación de las personas al someterlo a un proceso de anonimización”. En el aparte e.) debe indicarse ante quien se establece ese representante. d. En el artículo 57, consideramos oportuno advertir dado que el artículo que se indica en el numeral no concuerda con su contenido, que para el envío de mensajes para actividades electorales de los partidos políticos debe mediar consentimiento del titular (o en la línea incluso que lo ha establecido el TSE); y en el apartado 4. consideramos necesario incluir el plazo en que debe ser aplicada la solicitud del titular. e. Respecto al artículo 60, consideramos oportuno que se incluya lo referente al tratamiento de las (colegios profesionales, Dirección Nacional de Notariado y otros), sean por cuestiones disciplinarias o por atrasos en el pago de obligaciones; así como la publicidad que se le puede dar a esa información, el nivel de especificación y el tiempo de exposición. NOVENO: Referente al capítulo VIII de la Agencia de Protección de Datos Personales, el punto de partida es que debe consignarse en todo el documento el nombre correcto de la entidad, ya que incluso en el título del capítulo no se indica el nombre completo; otro punto relevante es que en otros países en donde ya cumplieron el proceso de adhesión al Convenio 108, 108 y protocolos, la autoridad no es un ente de desconcentración máxima sino que tiene una figura similar a la de una institución autónoma; si la figura de ente desconcentración máxima se mantiene las limitaciones que se señalan respecto a la autonomía se mantendrán independientemente del Ministerio al que se adscriba, pero esto es una decisión del legislador sobre la conveniencia de su ubicación. Sobre este capítulo indicamos que: a. La forma de contratación del personal no debe establecerse como una relación privada laboral. Esto trae una serie de inconvenientes de continuidad de la Institución en los procesos básicos de funcionamiento (financiero contable, proveeduría, recursos humanos, servicios de TI, asesorías técnicas, entre otros) y además de que la clasificación de puestos y salarios, no puede ser un acto discrecional, ya que debe optimizarse los recursos con que se dote la Agencia y la tendencia en el sector público es la unificación en materia salarial y la no creación de fueros especiales. Cabe destacar, que lo que debe existir es la modalidad de contratación por plazo determinado (no superior a 6 meses) de especialidades que se requiera para fortalecer procesos o para situaciones específicas, que pueden ir desde situaciones tecnológicas, legales o administrativas, hasta la necesidad de contratación de servicios por ejemplo de traducción para proyectos o procedimientos de	

		investigación que deba atenderse, lo cual debe referenciarse a un determinado cálculo del pago de servicios con el fin de que no se generen abusos. El contar con personal de apoyo capacitado (y con una clasificación de puesto acorde a las funciones) en los procesos permanentes de la Agencia, genera estabilidad, fortalecimiento de la Institución y evita decisiones arbitrarias que pueden comprometer la gestión. Aunado a esto si los requisitos del quien ejerza la Dirección se limitan a "reconocida competencia profesional, en particular en materia de protección de datos",(lo cual consideramos debe ampliarse dado que se trata de un gerente público y debería indicarse al menos una cantidad de años de ejercicio profesional y dirección de suspensiones ligadas al ejercicio de profesiones liberales equipos interdisciplinarios, entre otros); produce un problema a nivel institucional, ya que la Dirección no solo genera las acciones para el trabajo sustantivo en materia de protección de datos personales, sino que también es la responsable de todas las áreas de la misma, debiendo darle énfasis a la gestión presupuestaria, planes de compras, aprobación de estados financieros, aprobación materiales de divulgación y pautas publicitarias, control interno, SEVRI, planificación, entre otros; por lo que debe tener una experiencia amplia en gestión, no necesariamente en lo público, pero si preferiblemente parte de ella. Esto cobra importancia si se propone que el personal, pueda ser removido libremente, ya que al tener que cumplir con las obligaciones establecidas de cualquier otra institución pública y los plazos ya calendarizados, debe valorarse la continuidad en el servicio y el conocimiento de la normativa para el ejercicio y cumplimiento de sus atribuciones, incluso para no generar riesgos innecesarios en la gestión. Otro punto que debe recalcarse es no se contemplan prohibiciones legales e incompatibilidades del puesto de director, director Adjunto y del personal permanente y ocasional de la Agencia; ya que debe prevenirse situaciones de asesorías, contrataciones temporales y actividades posteriores al ejercicio de cargos dentro de la Agencia. Además, debe proveerse situaciones de impedimentos, recusaciones, excusas e inhibiciones, esto respecto a lo que establece el artículo 61.3. b. En lo que concierne al numeral 62 del régimen económico presupuestario debemos indicar que deben contemplarse los siguientes puntos: • Regla Fiscal: debe crearse la autorización que permita aumentar el tope por el monto del presupuesto aprobado en dicha ley, como excepción por una única vez, siendo que el presupuesto será mucho mayor y el primer año de conformación de la Agencia implicará compras, contrataciones y demás gastos mayores a los de años anteriores; ya que hay normas expresas que limitan este tipo de crecimiento presupuestario.	

		• Creación de plazas: debe crearse un transitorio de al menos dos años calendario en el cual la Agencia pueda solicitar todas las autorizaciones requeridas para el establecimiento de la nueva estructura, la creación y estudio de plazas de acuerdo a la nueva estructura. Este proceso debe atenderse de forma prioritaria, ya que implica el cumplimiento de los ciclos presupuestarios y los diversos trámites y tiempos de cada institución (Ministerio de Hacienda, MIDEPLAN). Esto debido a que las Normas de Ejecución Presupuestaria para el 2022 indican un impedimento al respecto Se recalca la necesidad de que a excepción del nombramiento del puesto del director y el del Adjunto, todos los demás puestos de la Agencia deberán ser incluidos bajo el Régimen del Servicio Civil. • Contrataciones adicionales: por disposiciones vigentes hay limitaciones para alquileres y compra de inmuebles, por lo que al requerirse un espacio físico mayor(al incrementar el personal), además del equipo tecnológico, de oficina y sistemas operativos administrativos y financieros, con el fin de cumplir con las funciones establecidas, sujetos a los procesos usuales de contratación administrativa, debe contemplarse para el primer ciclo presupuestario completo de la Agencia la adquisición o alquiler de una nueva edificación y aprovisionamiento correspondiente con el incremento de los contratos vigentes. • Ingresos: se considera importante indicar que, como órgano de desconcentración máxima y adscrito a un ministerio, de conformidad con la Ley No. 9524 articulo 1 (todos los presupuestos serán incorporados a presupuesto nacional para revisión, análisis y aprobación de la Asamblea Legislativa), la Agencia está sujeta a esta, por lo que todos los fondos que ingresen a la cuenta bancaria, por concepto de multas u otros, deben ser trasladados a la cuenta de la Caja Única del Estado, por lo que no integran de forma directa el presupuesto de la entidad, salvo que se establezca un mecanismo especial. • Cabe indicar que el Jerarca de la Institución a la que se encuentre adscrita la Agencia, tiene deber in vigilando sobre los recursos que ésta administra. (ver Dictamen C-052-2014 del 20 de febrero del 2014 de la Procuraduría General de la República) c. En lo que respecta a las funciones y potestades de la Agencia, debemos indicar: • Consideramos necesario que se conserve la atribución del numeral 16 inciso f, de la actual Ley. Y que, si bien consideramos conveniente que la Agencia no tenga un proceso de inscripción de bases de datos, si debe	

		contemplarse la notificación de existencia de ciertas bases de datos. • En cuanto a la función que indica " 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.", consideramos que en la práctica puede generar problemas de competencias y límites de las mismas; por lo que resulta más efectivo que se varíe a " Emitir criterios referentes a las medidas relativas a la protección de los derechos y las libertades de las personas físicas con respecto al tratamiento de datos personales, a las autoridades que lo soliciten", debiendo establecerse si ese pronunciamiento tendrá o no carácter vinculante • Se utiliza nomenclatura, como reclamaciones o diverso tipo de investigaciones, pero no dice claramente que será la instancia que tramitará los procedimientos por incumplimiento de las disposiciones de esta ley y establecerá las sanciones correspondientes, lo cual consideramos relevante se indique de forma directa y clara. • Debe incluirse un último apartado que indique y las otras atribuciones que le conceda esta ley, dado que en el texto de la misma se indican un sinnúmero de otras funciones que no están taxativamente en ese artículo. • Consideramos necesario se revise el numeral 64.f, para determinar si lo conceptuado se refiere a circulares o a otro tipo de documento jurídico. d. Respecto a la Dirección de la Agencia, consideramos que el numeral 65.2 debe indicar que son delegables tanto las funciones técnicas sustantivas de la Agencia como las administrativas; ya que en la práctica incluso resultaría más eficiente una labor complementaria entre lo sustantivo y lo administrativo, a compartir entre ambas figuras, sobre todo si no se establece una figura de director general Administrativo y Financiero, que en la práctica resulta más necesario. Adicionalmente respecto a la asignación de funciones al adjunto debe especificarse que quien ejerza la Dirección es quien asigna formalmente y en su ausencia temporal puede ejecutar todas las funciones. Un punto que debe mejorarse en la redacción es indicar que "no estarán sujetos a instrucción alguna en su desempeño", lo cual resulta contraproducente en la relación entre ambas figuras y entre estas y otros entes, en materias de gestión más no en lo que respecta a la protección de datos personales propiamente y es de carácter obligatorio cierto procesos de evaluación y control, como por ejemplo algo tan básico como la evaluación del	

		desempeño, la cual implica planificación, revisión y evaluación final de cumplimiento de metas y proyectos establecidos. Debe definirse desde la Ley la categoría salarial de ambas figuras o al menos un referente; ya que esto también define el resto de la estructura ocupacional de la Agencia. O indicarse expresamente en el transitorio que el salario del puesto de director continuará con la misma base y que de ahí se tome de referencia para el establecimiento de la nueva estructura. DÉCIMO: En lo que respecta al capítulo IX, consideran los que utiliza terminología que no es propia de nuestro medio y que puede prestarse a confusión; ya que por ejemplo indica que el procedimiento ante una posible vulneración, siendo que este término en la actualidad es utilizado cuando la base de datos en su totalidad o parte de esta, es accesada, sin autorización o de forma fraudulenta, más no se utiliza cuando se vulneran los derechos específicos de una persona, aunado a que se indica que el titular presenta una reclamación siendo lo más apropiado en este caso una denuncia. UNDÉCIMO: En el capítulo X consideramos necesario acotar: a. En el numeral 72, debe incluirse una opción que indique como sujeto responsable “cualquier persona que realice tratamiento de datos personales”, esto con fines de facilitar el establecimiento de responsabilidades dentro de los procedimientos. b. Respecto al artículo 73 debe definirse a cuál salario base se refiere y cuál será la referencia para actualizar el monto. c. En las causales de sanción debe establecerse un último apartado en cada tipo que indique otras acciones que a criterio de la Agencia pueda considerar de ese nivel de falta, previo análisis de los hechos denunciados y de la prueba recabada. Así mismo debe indicarse expresamente como sancionable el no cumplimiento de las órdenes emanadas de la Agencia para el acceso, rectificación, cancelación, oposición y portabilidad en un caso concreto; así como de las disposiciones que de esta emanen. d. Debe clarificarse en la propuesta los plazos de prescripción, el conteo de los mismos, la interrupción, el inicio de plazos, así como diferenciarlo de la caducidad; ya que en el proyecto se confunden ambas figuras y no es clara la aplicación de las mismas. e. En el artículo 78.j debe indicarse por cuánto tiempo puede tomarse como reincidencia para el establecimiento de la sanción, ya que por debido proceso no puede dejarse indefinido. f. En el numeral 79.3, debe indicarse que la Agencia propondrá la iniciación de las actuaciones disciplinarias, pero es responsabilidad del Jerarca la tramitación o no del procedimiento correspondiente.	

		DUODÉCIMO: Los capítulos IX y X sobre el "Procedimiento en caso de posible vulneración a la normativa de Protección de Datos y el Régimen Sancionatorio", mantiene vigente una problemática que experimenta actualmente la Agencia al tramitar los procedimientos establecidos por el legislador, ya que, la actual legislación cuenta con dos procedimientos, el primero de Protección de Derechos y el segundo el Procedimiento Sancionatorio (en que se establecen sanciones), lo que implica, que se alargue la posibilidad de sanción efectiva; lo recomendable sería contar con un único procedimiento ordinario (el cual deberá cumplir todas las garantías del debido proceso), y si el titular lo solicita establecer una medida cautelar mientras se resuelve el expediente sobre el fondo tanto respecto a la protección de derechos como a la sanción; lo que permite cumplir de forma efectiva, expedita y eficaz con lo establecido en la ley, sin etapas innecesarias, tomando en consideración que se le darán a la Agencia los recursos para el cumplimiento de sus fines. Este procedimiento debe definirse si se establece como uno especial o si se referencia directo a la Ley General de la Administración Pública. Se considera sobre los transitorios, que la entrada en vigor no debería ser a partir de la publicación, sino doce meses después y que esa sería la fecha máxima para que éste emitida la reglamentación necesaria y también es un tiempo prudencial para el ajuste de procedimientos a nivel de quienes realizan tratamiento de datos personales. Debe tomarse en consideración, incluso, que la contratación de los Oficiales de Protección de datos personales de acuerdo con las consideraciones técnicas legales no es un proceso sencillo, ya que como se indicó no existen datos exactos respecto a la posibilidad que tiene el mercado laboral para solventar la cantidad de personas físicas y/o jurídicas suficientes que cumplan para asumir esos roles.	
CTCR-2022-0282	Colegio de terapeutas	Manifiestan su apoyo al proyecto	11 de agosto del 2022
MEIC-DM-OF-340-2022	Ministerio de Economía, Industria y Comercio	Este Ministerio no encuentra objeciones que impliquen traslapes de responsabilidades o competencias, y no se observa interferencia o colisión de las potestades funcionales de esta "nueva ley" de protección de datos" con las obligaciones del MEIC	09 de agosto del 2022

CIT-0038-2022	INFOCOM	INFOCOM desea indicar que, en términos generales, se encuentra a favor de este proyecto de ley; y no omite manifestar que, aunque se apoye la iniciativa, considera necesaria la mejora de ciertos artículos y la inclusión de algunos temas para perfeccionar el alcance de la iniciativa. • Es importante mencionar que la Cámara considera fundamental que el proyecto establezca una mejora y fortalecimiento de la estructura y capacidades institucionales de la Agencia de Protección de Datos Personales (PRODHAB). Se considera necesario promover la competitividad e innovación del país, por lo que se apoya la conveniencia de trabajar en la reforma integral a la Ley N° 8968. La norma vigente, no contempla todos los principios, derechos, ni bases de legitimación, que en materia de protección de datos personales sí se encuentran reconocidos en las legislaciones más maduras y que son referencia para Costa Rica. Nuestro país debe contar con un marco adecuado en materia de protección datos, siendo esencial el dotar de mayor autonomía, e independencia práctica y jurídica, al órgano rector, sea a la Agencia PRODHAB; de manera que ésta pueda garantizar efectivamente los derechos y libertades de los titulares. Por medio de las reformas necesarias en esta materia, nuestro país se acerca a los estándares internacionales, buenas prácticas, y a los instrumentos desarrollados por los estados iberoamericanos y la Comunidad Europea. • Desde INFOCOM, nos ponemos a disposición de esta Comisión Legislativa, como representantes de la industria de telecomunicaciones y tecnología, con nuestro criterio técnico especializado, para ampliar la posición sobre las observaciones hechas a este proyecto de ley; poniéndonos a las órdenes para acudir en audiencia, en caso de que la Comisión lo 2considere pertinente, y tener la oportunidad de externar e intercambiar impresiones sobre la materia. II. OBSERVACIONES ESPECIFICAS SOBRE EL TEXTO DEL PROYECTO DE LEY 1. En general, se sugiere que los principios que se observen en esta normativa, para el tratamiento de datos personales, sean los siguientes: “principios de exactitud, legitimación, lealtad, transparencia, limitación de la finalidad, minimización de los datos, limitación del plazo de conservación, responsabilidad proactiva, seguridad, integridad y confidencialidad.” 2. Algunos artículos, como el ARTÍCULO 2. Definiciones: inciso m). Grupo empresarial; o el ARTÍCULO 6. Ámbito de aplicación territorial. Inciso 4); y el ARTÍCULO 10. Tratamiento de datos personales sensibles. Inciso b): Conviene que se aclaren en sus definiciones, por ejemplo, para poder comprender el concepto de “grupo empresarial” (Ver definición de “grupo económico” de la Ley 9736); y evitar interpretaciones sobre	22 de agosto del 2022

		su alcance. 3. En el ARTÍCULO 11. Tratamiento de datos personales relativos a condenas e infracciones penales. Inciso 1): Se sugiere verificar si es más bien el Ministerio de Justicia, el que lleva el registro de las condenas penales de las personas que tienen procesos de ejecución de pena con medidas alternativas 4. ARTÍCULO 14- Principio de exactitud: En casos como el del inciso 1), subinciso b): No es una causal de exclusión de responsabilidad en relación de los principios. Le corresponde al responsable rectificar. 5. ARTÍCULO 15 - Principio de legitimación: El tratamiento no solo lo realiza el responsable, por lo que la recomendación es que quien haga tratamiento, tenga una base de legitimación. Sobre el inciso c): Debe haber una norma habilitante para el tratamiento, lo contrario debería ser excepcional. Se podría prestar para muchos tratamientos " por ser considerados una facultad propia". La limitación del derecho debe ser excepcional. Adicionalmente, sobre los dos últimos párrafos del Art. 15, se considera, sobre el tratamiento de datos personales de contacto que sea imprescindible para la localización de personas físicas que prestan sus servicios al responsable, que esto no es necesario disponerlo; ya existe la base de legitimación del contrato y puede ser confuso, incluso con geolocalización, la cual está sujeta a una serie de condiciones, porque debe ser mínimamente invasiva. Lo dispuesto es Innecesario, pues ya existe la base de legitimación de interés público y la obligación legal. Agregar párrafos adicionales, se puede prestar para confusiones. 6. ARTÍCULO 16. Condiciones para el consentimiento: Sobre la “acción afirmativa clara”, se sugiere incluir este concepto en las definiciones. 7. ARTÍCULO 24. Principio de seguridad. Inciso 6): Lo dispuesto en este artículo, podría reñir con las competencias que tiene el MICITT en la materia. Debe revisarse el ámbito de competencias de la Agencia Nacional de Gobierno Digital, la cual también tiene funciones en esta materia. 8. ARTÍCULO 25. Notificación de vulneraciones a la seguridad de los datos personales: Se sugiere clarificar el manejo confidencial de estos datos. 9. ARTÍCULO 36. Ejercicio de los derechos ARCO y de portabilidad. Inciso 2), subinciso b): Se sugiere agregar, a efecto de evitar subjetividades e interpretaciones: “autoridades expresamente establecidas en la ley.” 10. ARTÍCULO 40. Encargado de tratamiento. Inciso 6): De esta norma, pareciera interpretarse que para que existan encargados de tratamiento en el sector público, se va a requerir una nueva Ley, sobre todo pensando de cara a las instituciones autónomas. Se sugiere que, en el caso de las autónomas, se incluya un capítulo que regule la materia, y en el caso del Gobierno Central, indicar que la regulación se realizará mediante Reglamento. 11. Sugerimos que, a lo largo del texto del proyecto, cuando se haga referencia a la “Ley 7494, Ley de Contratación Administrativa, de 2 de mayo de	

		1995 y su reglamento", se modifique para adaptarlo a la referencia de la nueva "Ley General de Contratación Pública, N° 9986, del 27 de mayo del 2021 y su reglamento". l2. ARTÍCULO 47- Privacidad por diseño y privacidad por defecto. Inciso 1): Se considera importante incluir las condiciones que se deben tomar en consideración para aplicar privacidad desde el diseño. 13. En cuanto a los ARTÍCULOS 48 y 49, sobre el Oficial de protección de datos personales y su Intervención: Sugerimos incluir a la Asamblea Legislativa; y revisar los plazos amplios brindados para el caso de reclamaciones ante la Agencia PRODHAB, para reducir estos plazos (incisos 1 y 2 del Art. 49) 14. ARTÍCULO 51 - Evaluación de impacto a la protección de datos personales. Inciso 6): Sobre la disposición para recabar la opinión de los titulares o de sus representantes en relación con el tratamiento previsto: Se hace la observación de que este tipo de disposiciones corresponden más en relación con códigos de conducta. Sobre el procedimiento previsto al final del inciso 6) y en el inciso 7), para que 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: Se sugiere incluir un artículo separado sobre la consulta previa, e incluir los requisitos mínimos en el mismo artículo. 15. En el ARTÍCULO 63. Funciones. Inciso c): Se sugiere sustituir el concepto de "asesorar", por "emitir criterio". Agradecemos tomar en cuenta las anteriores observaciones y consideraciones sobre este proyecto de ley consultado. Reiteramos la disposición desde INFOCOM, para ampliar con nuestro criterio técnico especializado, esta posición; o bien acudir en audiencia ante esta estimable Comisión.	
No detalla	Cámara de Tecnologías de Información y Comunicación	ANÁLISIS DE FONDO Y FORMA ARTÍCULO 2 Cita textual: 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	08 de agosto del 2022

		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 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. Observaciones: · Inciso h: Provee una definición demasiado amplia de datos sensibles por lo que puede provocar inseguridad jurídica. Esta es una categoría que supone una mayor diligencia y restricciones para su tratamiento por lo que es fundamental tener esa seguridad jurídica Inciso u: Sugerimos eliminar el concepto de transmisión en la definición de transferencia de datos para evitar confusiones entre ambos conceptos transmisión y transferencia. Recomendación de enmienda: Se sugiere que la lista incluida en el artículo no sea enunciativa sino taxativa. Además, se recomienda la eliminación del concepto de “transmisión” en el inciso u. ARTÍCULO 6Cita textual: 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. Observaciones: El inciso c resulta superfluo puesto que el acuerdo es válido por la sola voluntad de las partes (principio de autonomía), sin requerirse que una norma específicamente lo reconozca. Algo similar ocurre con las normas del derecho internacional privado, toda vez que es materia regulada por Tratados Internacionales que no pueden ser modificados por una norma local El inciso d, básicamente impone el derecho local a quien contrata un proveedor de servicios o un Encargado de tratamiento en el país (por ejemplo, para hosting o procesamiento de datos). En esos escenarios, debería ser únicamente el encargado de tratamiento quien esté sujeto a la normativa local, no el responsable, que simplemente elige contratar a alguien en nuestro país. La redacción además parece contradecirse con el mismo artículo, que indica: “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” Invitamos a reflexionar el impacto que esto puede tener en la industria de servicios de Back Office y de almacenamiento de datos en nuestro país. Recomendación de enmienda: Se sugiere la eliminación de los incisos c y d. Se sugiere además incluir únicamente los escenarios que	

		contiene el RGPD (Reglamento General de Protección de Datos de la Unión Europea) ARTÍCULO 10 Cita Textual: 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 supuestosa. 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. Observaciones: Se hace referencia a conceptos indeterminados que pueden conducir, de manera consuetudinaria, a la aplicación de la discrecionalidad, de lo que podría derivar vicios de legalidad y/o contraposición a los principios que pretende regular la ley. Recomendación de enmienda: Se establecen dos posibles vías de enmienda o aclaración, las cuales se detallan a continuación: 1. Respecto a los datos sensibles: Se considera importante que la excepción a la prohibición de su tratamiento considerada en el inciso d) quede así: "Se cuente con el consentimiento expreso del titular o que éste haya dado el consentimiento en el marco de un contrato donde su tratamiento es necesario". De otro lado, se reitera que es fundamental acotar la definición de esta categoría ARTÍCULO 22 Cita Textual: 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. Observaciones: Los datos pueden conservarse en virtud del interés legítimo del responsable, por ejemplo, por razones de seguridad informática (el borrado de los datos puede afectar los algoritmos destinados a detectar amenazas cibernéticas) Recomendación de enmienda: Se recomienda incluir una referencia al interés legítimo del responsable en la conservación de los datos más allá del tiempo requerido para el cumplimiento de la finalidad originaria. ARTÍCULO 25 Cita Textual: 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, aun 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. Observaciones: Se sugiere delimitar el alcance de las notificaciones por vulneraciones de la seguridad de los datos personales, adoptando para ello un enfoque basado en el riesgo y naturaleza del dato. Este enfoque garantiza que los supuestos y requisitos para notificar vulnerabilidades de datos sean considerados a la luz del probable riesgo en los derechos de los titulares de los datos.	

		Asimismo, respecto al periodo establecido para notificar a la autoridad se sugiere adoptar una redacción más cercana al reglamento europeo que contempla no más de 72 horas, pero también la posibilidad de exceptuarse este plazo debiendo el responsable identificar las razones del retraso. Lo anterior, pues estos incidentes de seguridad pueden ser de alta complejidad y requerir de un plazo adicional para su remisión a la autoridad. ARTÍCULO 33 Cita Textual: 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 decisión4. 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. Observaciones: Este artículo plantea una restricción al uso de decisiones individuales automatizadas en el marco de un contrato así: “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.” Esta limitación no corresponde con la normativa internacional y puede limitar la utilización de avances tecnológicos benéficos por ejemplo en relaciones de consumo afectando la experiencia de consumo. Es claro que en el inciso primero de este artículo indica cuándo una decisión no puede ser tomada únicamente con mecanismos automatizados, esto es, cuando tenga efectos jurídicos o significativos. El inciso arriba citado por el	

		contrario puede generar una obligación desproporcionada al responsable de los datos de garantizar siempre la intervención humana en decisiones sin ninguna trascendencia para el titular y que superan la racionabilidad o lógica del uso automatizado en primer lugar El otro componente crítico de este artículo es la importancia de moderar el derecho a acceder a una explicación con los derechos de los terceros o del responsable. Así un ajuste en este sentido podría atender tal preocupación. Recomendación de enmienda: El otro componente crítico de este artículo es la importancia de moderar el derecho a acceder a una explicación con los derechos de los terceros o del responsable. Así un ajuste en este sentido podría atender tal preocupación. Recomendación de enmienda: se recomienda buscar una redacción alterna para el inciso 3, así como para el artículo 59, 63, 72. Finalmente consideran que en general el proyecto se alinea al estándar del Reglamento europeo GDPR.	
SJG-1563-08	Junta de Gobierno del Colegio de Médicos y Cirujanos	No detallan criterio	11 de agosto de 2022
COCR-174-2022	Colegio de Optometristas de Costa Rica	Hacen algunas observaciones menores, y su mayor preocupación se centran en el capítulo VII relativo a Disposiciones aplicables a tratamientos concretos en el cual estima importante la naturaleza jurídica que se le brinda a la PROHAD, pero si llaman la atención en orden de montos fijados para las multas, recomiendan revisar los montos.	22 de agosto del 2022
PICQPA027-2022	Colegio de Ingenieros y Profesionales Afines	Igual que el Colegio de Optometristas de Costa Rica les preocupa el capítulo de sanciones el cual las consideran desproporcionadas e irracionales.	05 de agosto del 2022
CTS-278-2022	Colegio de Trabajadores Sociales	“En efecto este proyecto constituye una vigorización en la protección de datos de personas”. Por ende, este Colegio Profesional apoya este proyecto.	02 de diciembre del 2022
CPPCR-JD-152-2022	Colegio de Profesionales en Psicología	Este colegio sugiere agregar en el artículo 17, inciso 2, lo establecido en el artículo 46 del Código de la Niñez y Adolescencia, en cuanto a la denegatoria del consentimiento. Igualmente pide aclaraciones de redacción en artículo 2, 8 y 10.	13 de diciembre del 2022
DFOE-GOB-0477	Contraloría General de la República	Sugieren revisar el inciso 6) del artículo 24. También hacen alusión al artículo 61 del proyecto, que establece la estructura administrativa que tendría la Agencia de Protección de Datos como un órgano con desconcentración máxima y personalidad jurídica instrumental que se traslada al MICITT, Asimismo, se indica que el reconocimiento de la personalidad jurídica instrumental genera que en la práctica los órganos desconcentrados operen como entidades distintas e independientes que no responden a un direccionamiento integrado por parte de los jerarcas, lo que desnaturaliza su esencia como órganos	29 de noviembre del 2022

		parte de una entidad mayor, inclusive en temas de rectorías. En el tema presupuestario, se mantiene la necesidad de realizar un análisis técnico y presupuestario para la agencia regulado en el artículo 62. Así mismo, mantienen las observaciones referentes a las potestades de fiscalización relacionadas con el artículo 8. Finalmente, se mantiene las observaciones realizadas en relación al artículo 65 el cual regula los aspectos sobre la Dirección de la Agencia de Protección de Datos y la remoción de la dirección.	
1044-DG-2022	Organización de Investigación Judicial (OIJ)	Hacen algunas observaciones de forma a los artículos 16, 16, inciso 4), artículo 24, ítem 2, inciso b), artículo 63 inciso c, artículo 65, artículo 65 inciso a), artículo 74, artículo 75 y artículo 77	06 de diciembre del 2022
P-001-2023	Cámara de Comercio de Costa Rica	Hacen consideraciones al artículo 2, artículo 6, artículo 10, artículo 16, artículo 20, artículo 25, artículo 28, artículo 29, artículo 62, artículo 73.	09 de enero del 2023
APD-086-12-2022	Agencia de Protección de Datos de los Habitantes	Hizo una serie de observaciones a los artículos 2, inciso l y artículo 12. Sobre varios incisos del artículo 2, también artículo 4, artículo 8, artículo 13, artículo 19, artículo 25, artículo 45, artículo 4, artículo 55, y artículo 63	02 de diciembre del 2022
SP-250-2022	Corte Suprema de Justicia	Indican que el texto sustitutivo si afecta la organización y funcionamiento del Poder Judicial, toda vez que se requiere reorientar la asignación de recursos humanos, financieros, tecnológicos y otros, para la adecuada gestión de las distintas técnicas internas que habrían de asumir las distintas funciones y deberes previsto en esta Ley.	12 de diciembre del 2022
MIDEPLAN-DM-OF-2368-2022	MIDEPLAN	Hacen una serie de observaciones de fondo importantes al presente proyecto de ley que son específicamente: 4. **Análisis del articulado:** 4.1. Artículo 2, inciso h), Definiciones, se recomienda incluir en el párrafo, el atributo de “condición socioeconómica” que se incluye en la actual definición de la Ley N°8968. Asimismo, no se incluye en el punto 1 del artículo 10 en el listado de atributos, a modo de homologar el uso conceptual por lo que es recomendable su inclusión. 4.2. Artículo 8, punto 4 se habla de que las cesiones de datos deben documentarse mediante convenio interinstitucional y que debe ser comunicado a la Agencia de Protección de Datos Personales, los cuales deben ser publicados, pero no se indica el medio o espacio a ser publicado (La Gaceta, página oficial del responsable, página oficial de la Agencia, etc.) o a quién le corresponde publicarlo, lo cual se considera importante especificar a modo de transparencia y de documentar el mandato en la ley Además, se muestra que dicha cesión será publicada para que sea sometida a escrutinio de la ciudadanía, pero no se menciona la finalidad del escrutinio de un convenio interinstitucional, ya que; al ser un tipo de consulta debe contar con un objetivo, un mecanismo que lo respalde y un público meta, aspectos que no se encuentran indicados en la propuesta y es significativo dejar constatado.	02 de diciembre del 2022

		4.3. Artículo 19, Principio de transparencia, se considera acertado lo especificado en el texto, pero preocupa que no quede claro quién o qué entidad (si será la Agencia) garantizará que efectivamente el Responsable cumplirá con lo estipulado en el principio ya que bajo el escenario de que el responsable no comunique la información al Titular y el Titular por ende, no conozca con antelación sobre la existencia de sus datos personales en manos del Responsable, no se plantea un mecanismo que haga efectivo el principio en cuestiones de trazabilidad y de responsabilidad de las partes 4.4. Artículo 22, Principio de exactitud, punto 2, se recomienda especificar el procedimiento para comunicar al Titular cómo y cuándo se realizará la eliminación o supresión de sus datos, en poder del Responsable, ya que no se menciona en el texto. 4.5. Artículo 23, Principio de responsabilidad proactiva, lo indicado en el punto 4 en cuanto a que el Responsable revisará y evaluará los mecanismos adoptados para cumplir con dicho principio, salta la necesidad de encontrar en el articulado una competencia que parece ser de la Agencia pero que no se está contemplando en ninguno de los artículos, el cual consiste en incluir que el Responsable deberá coordinar con la Agencia cualquier requerimiento, solicitud o capacitación que requiera al respecto, entendiendo que este tema conlleva una etapa de preparación muy importante y muchos cuerpos institucionales públicos y privados no tienen el conocimiento ni las pautas claras de lo que implica el tema, por lo que debe fortalecerse este rol asesor de la Agencia con respecto a las instituciones o Responsables involucrados, siendo así que se recomienda considerar este aspecto como una competencia de asesoría y capacitación por parte de la Agencia a los enlaces Responsables. 4.6. Artículo 25 sobre la notificación de violación a la seguridad de los datos personales se recomienda valorar de manera adicional en el listado del punto 4, el posible riesgo o afectación de la vulneración de la salida de los datos personales, siendo esto un derecho del Titular a conocer el destino y posibles efectos que sus datos personales puedan acontecer. 4.7. Artículo 29, Derecho de acceso, en el punto 5, se recomienda incluir en la propuesta lo que se entenderá en la ley como una “causa legitima”, la cual será eventualmente lo que respalde al Responsable al momento de responder al Titular cuando pida acceso a sus datos, de tal forma que no quede a la subjetividad o se incurra en disparidades al momento de emitir criterio dentro del mismo sector público. 4.8. Artículo 37, Obligaciones del Responsable del tratamiento, se recomienda considerar agregar en el listado como una obligación del Responsable la de “informar al Titular sobre las obligaciones y responsabilidades que tiene como Responsable ante el tratamiento de sus datos, así como posibles riesgos y medidas de mitigación y actuación que considera el Responsable al tener en su poder los datos personales del Titular.” 4.9 Artículo 40, Encargado de tratamiento, punto 6,	

		no se comprende en cuanto a redacción la frase: “En el ámbito del sector público podrán atribuirse las competencias propias de un Encargado del tratamiento a un determinado órgano de la Administración Pública…” en el tanto no se sabe si cada institución pública a partir de esta ley podrá “atribuirse” el ser encargado del tratamiento de los datos, o se designará a un ente de manera especial dicho tratamiento en virtud de toda la administración, algo como un centro de tratamiento de datos personales Es sustancial valorar la redacción actual del artículo en el punto específico, así como la intencionalidad de incluirlo en la propuesta. 4.10 Artículo 44, Bloqueo de datos, se recomienda cambiar las palabras “Administraciones Públicas” por “instituciones”, siendo que el concepto del primero es muy claro según diversos dictámenes de la PGR, mientras que instituciones al ser más genérico torna inclusivo el ámbito organizacional al que se refiere. 4.11 A partir del artículo 48 se regula lo referente a una figura nueva denominada Oficial de protección de datos personales. Dicho artículo señala el tipo de entidades públicas y/o privadas donde debería estar fungiendo este oficial. Aunque se entiende la idea de tener un responsable sobre el tema en cuestión, no parece que sea la mejor forma nombrar o responsabilizar a una figura para dicha situación. Los principios de protección de los datos personales giran alrededor de la responsabilidad de toda la administración pública, en virtud del liderazgo de las jerarquías en hacer respetar la ley. Ahora bien, cuando se trata de los responsables del tratamiento de datos, éstos deberían adoptar e implementar medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con la legislación nacional. En este caso, al menos para el sector público, tal parece que más que nombrar responsables u oficiales del tema, es más proclive a mejores resultados que por medio de directrices, mecanismos de gestión, habilitaciones en sitios web o aplicaciones, se tomen las medidas para las funciones que fueron encargadas. En ese sentido, un reclamo ciudadano por un caso de este tipo no necesita un oficial que tramite: lo que se necesita es una plataforma que sea práctica para poder gestionar dicho reclamo y sea rápida la forma de tramitar y resolver. Por lo tanto, esto no se resuelve con un oficial, se resuelve con una adecuada administración que permita resolver las distintas disconformidades que puedan surgir. Igualmente, no se muestra en el articulado si esta figura será un puesto creado como nuevo en el sector público, si son puestos que ya funcionan como tal o si se considera un recargo de funciones a una figura similar que ya exista en el sector público, lo cual es de relevancia resaltar en el presente criterio, ya que la consideración de una figura como esta debe ser vista a la luz de la disponibilidad de recursos presupuestarios para el efecto y el criterio de oportunidad y	

		disponibilidad con que cuente la institución pública para asumir una figura como esta, en caso de que así sea. 4.12 Artículo 51 sobre evaluación de impacto, en el punto 2 se menciona que el Responsable del tratamiento realizará la evaluación de impacto relativa a la protección de datos, lo cual presupone que sería una tarea asignada al oficial de protección de datos, elemento que refuerza la importancia de definir y dotar de herramientas al oficial tanto en formación como de gestión para llevar a cabo esta función. En ese mismo artículo, en el punto 6, se exterioriza que el Responsable consultará a la Agencia de Protección de Datos antes de proceder al tratamiento cuando se indique alguna muestra de riesgo posterior a una evaluación de impacto, lo cual pareciera indicar que se debe crear un modelo de evaluación y un sistema de riesgos alrededor de la propuesta, así como un responsable de crearlo y por tanto de darlo a conocer, pero no se indica si estos criterios de evaluación serán dados por la Agencia o queda a criterio de cada institución su creación, por lo que se recomienda valorar este aspecto en función de la importancia del tema y su sensibilidad. 4.13 Artículo 61, Disposiciones generales. Sobre la naturaleza jurídica propuesta a la Agencia, existen varias distorsiones con algunos temas propuestos. A la Agencia se le establece desconcentración máxima del MICITT con personalidad jurídica instrumental. Se entiende según las competencias que se establecen que se pretende contar con un órgano que pueda actuar sin presión del ministro, de manera que pueda ejercer su trabajo con independencia técnica sin que sus decisiones sean revisadas por el jerarca. No cabe la menor duda que es un panorama adecuado, si no fuera porque actualmente existe una Agencia, con desconcentración máxima y con personalidad jurídica que prácticamente opera con el mismo modelo, pero que ha demostrado bajo o nulo impacto en la protección de datos de los habitantes. En ese sentido, sin el menor ánimo de describir o valorar la gestión o lo realizado hasta el momento por la PRODHAB, queda la duda del por qué plantear un órgano con la misma naturaleza jurídica, siendo que prácticamente tiene los mismos atributos y que no parece que la independencia de criterio o el manejo presupuestario independiente sean elementos que hayan sido fortalezas de este órgano desde su fundación en 2011 por medio de la ley que justamente este proyecto pretende derogar. 4.14 Artículo 62, Propuesta de régimen económico presupuestario, no queda claro que la transferencia procedente del presupuesto nacional de la República, que corresponda al menos a cinco mil trescientos nueve, cero cinco (5 309,05) salarios base, sea lo idóneo para poder operar según las competencias establecidas; Es decir, se necesita el contraste con el financiamiento actual de la PRODHAB -por ejemplo- para saber si operativamente se sostiene. En este mismo artículo, pese a mencionarlas, existen algunas inconsistencias con la Ley “Fortalecimiento	

		de las Finanzas Públicas, N°9635 de 3 de diciembre de 2018" al contraponerse con la Ley de "Fortalecimiento del control presupuestario de los órganos desconcentrados del Gobierno Central, N°9524 de 7 de marzo de 2018"; entre ellas, el atribuir la personalidad jurídica instrumental y señalar que será la Contraloría General de la República quien fiscalizará su presupuesto. Al respecto de la Ley N°9635 se menciona sobre la asignación presupuestaria a este tipo de órganos desconcentrados lo siguiente "Artículo 19: En el caso de los recursos para los órganos desconcentrados, el ministro de Hacienda decidirá, mediante criterios de suficiencia fiscal, el respeto a los derechos fundamentales y siguiendo las prioridades del Plan Nacional de Desarrollo, el monto a presupuestar a estos órganos y su crecimiento." Por lo que se recomienda valorar nuevamente lo dispuesto en el proyecto en términos de presupuesto y finanzas bajo la normativa nacional vigente, ya que existe cierta confusión entre lo señalado entre los puntos a, b y c de dicho artículo. 4.15 Artículo 63 inciso j), Funciones; Una de las funciones de la Agencia, es "Fomentar el uso de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos", lo cual crea la duda de si eventualmente podría afectar de alguna manera el trabajo que ya realiza la Dirección de Certificadores de Firma Digital del MICITT en materia de firma digital, o si bien podría terminar generando una duplicidad de funciones. Lo anterior tomando en cuenta que, entre las funciones de tal Dirección, según el artículo 24 inciso b) de la Ley "Ley de Certificados, Firmas Digitales y Documentos Electrónicos", N°8454 de 30 de agosto de 2005, se encuentra "Llevar un registro de los certificadores y certificados digitales" y "Fiscalizar el funcionamiento de los certificadores registrados, para asegurar su confiabilidad, eficiencia y el cabal cumplimiento de la normativa aplicable, imponiendo, en caso necesario, las sanciones previstas en esta Ley". 4.16 En el inciso g) del artículo 63 se propone "Cooperar compartiendo información con otras autoridades de control y prestar asistencia mutua en materia de protección de datos". Si bien en la ley no se hace mención al concepto de interoperabilidad, es posible firmar que la función recién descrita es análoga a dicho término, al menos como es entendido en la Ley "Creación de la agencia nacional de Gobierno Digital"4N°9943 de 11 de mayo de 2021, ya que entre los objetivos de la Agencia Nacional de Gobierno Digital se encuentra "Implementar mecanismos de intercambio de información, identidad digital e integración de los sistemas de información electrónica (interoperabilidad), con el propósito de facilitar los servicios al ciudadano y generar ahorros significativos para la Administración Pública, la ciudadanía y las empresas", surge la duda de si la anterior disposición puede afectar el trabajo de la ANGD o generar duplicidades. 4.17 El inciso c) del mismo artículo menciona que entre las funciones de la Agencia también se encuentra "Emitir	

		criterio sobre la protección de los derechos y las libertades de las personas físicas con respecto al tratamiento de datos", tampoco queda claro cuál sería la relación entre el órgano propuesto y el CSIRT-CR, ya que este último tiene como objetivo, según el Decreto Ejecutivo "Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR", Nº37052-MICIT de 9 de marzo de 2012, artículo 2, "Incentivar, orientar y promover las iniciativas públicas y privadas conducentes a lograr un adecuado desarrollo del país en el campo de la seguridad de las tecnologías de la información y la comunicación, esfuerzos orientados a lograr una mayor protección del ciudadano". En ese sentido, sería proactivo establecer dentro de la ley un mecanismo de coordinación entre ambos entes para potenciar sus esfuerzos en materia de ciberseguridad. Esto conlleva a que se redacte con más precisión algunas de las funciones señaladas que serían total responsabilidad de la Agencia. 4.18 Artículo 64- Potestades. Podría haber inconsistencias entre el ámbito de acción propuesto para la ley, y las posibilidades reales que se exponen en este artículo, siendo que se plantea que un órgano desconcentrado de un ministerio realice funciones que pueden rayar con la constitucionalidad. Es decir, podría verse limitada la Agencia a solo poder realizar sus funciones en una parte de la Administración Pública, siendo que no le alcanza su naturaleza jurídica para poder llegar a otras entidades y organismos privados. Es importante recordar que el ámbito de acción de la ley, aunque mantiene gran amplitud, lo cierto del caso es que es limitado el ámbito que podría tener un órgano desconcentrado de un Ministerio, que normalmente solo puede llegar a tener incidencia en otras instituciones del Gobierno Central (por ejemplo, en caso de querer realizar auditorías de protección de datos o bien realizar inspecciones en equipos y medios de tratamiento de datos). 4.19 Artículo 65- Dirección de la Agencia de Protección de Datos. Existen algunas inconsistencias. Se rescata como positivo que el Jerarca de la Agencia sea unipersonal y no un órgano colegiado, ahora bien; dicho Director debería responder directamente al Jerarca ministerial, en este caso al Ministro del MICITT. No obstante, se construye un procedimiento complicado que no atiende el mandato que se pretende desde el Gobierno Central, la orientación que pueda dar el Ministerio a su órgano desconcentrado. En ese sentido, todo el proceso de selección y validación, inclusive del nombramiento del Director, es impropio al espíritu que pretende la Ley General de Administración Pública en cuanto a la jerarquía de los órganos desconcentrados. Justamente en el trámite o procedimiento de evaluación del mérito por parte de la Asamblea Legislativa, se mezclan formas de nombramiento impropias para un órgano desconcentrado que finalmente es parte del Gobierno Central como cualquier otro de los más de 60 órganos desconcentrados a Ministerios que responden a una orientación específica del Poder	

		Ejecutivo. Es justo acá donde se evidencian problemas entre lo que se pretende con la Agencia, y la naturaleza jurídica que se le asigna. No se recomienda un nombramiento de este tipo para la Dirección de la Agencia. El nombramiento y remoción del Director de la Agencia debe ser responsabilidad de quien ostente la jerarquía del MICITT. No debe pasar por procesos de validación o evaluación por otras instituciones. Este tipo de procedimientos no son para órganos desconcentrados, y parece que responde más a órganos auxiliares del Poder Legislativo -en los cuáles sí existe validación y nombramiento de parte de los diputados de la República-. Además, en cuanto a los términos utilizados en este artículo, relacionado a la Dirección y el Adjunto, en el caso del primero sería lo más conveniente referirse a la persona en el cargo de "Director" y no a una unidad administrativa "Dirección" y en cuanto a lo mentado como "Adjunto", lo más conveniente sería tratarlo como un cargo de "Subdirector". 4.20 A partir de los artículos 66-80 se detalla el régimen de reclamaciones ante posibles vulnerabilidades a la protección de datos, el tipo de sanciones, daños entre otros. Aquí se expone parte de la actuación que tendría la Agencia y es donde vuelven a presentarse inconsistencias ya que parece que en ocasiones actúa como un Tribunal Administrativo, ya que a nivel competencial la intención pareciera crear un órgano de corte Tribunal Administrativo, que estaría desempeñando procedimientos legales que normalmente concluye en la emisión de una decisión sancionatoria. Se observan potestades en estos artículos que parece procuran resolver impugnaciones que se presenten contra determinados actos administrativos. Si bien este tipo de labor no es materia exclusiva de un Tribunal Administrativo, al observar distintas potestades, funciones y atribuciones que se le han dado a lo largo del proyecto a la Agencia, tal parece que también responde a este tipo de actuaciones que tienen los tribunales dentro de la organización del Gobierno Central. El tema en cuestión es que finalmente la Agencia no es un Tribunal, y de cierta manera mezcla atribuciones que eventualmente se perciben a lo largo del proyecto. 4.21 Artículo 79- Este artículo, faculta a la Agencia para sancionar las infracciones de los responsables y encargados de tratamiento de datos personales de una serie de entidades distintas, lo cual podría generar roces de constitucionalidad al entrar en posible conflicto con la división de poderes y con la autonomía de instituciones autónomas. En el primer caso, debido a que la aplicación del artículo incluye al Poder Legislativo, al Judicial y al TSE. En el segundo caso, porque también incluye a las municipalidades, universidades públicas y la Administración Pública Descentralizada en general. En ese sentido se reitera que, en tanto órgano desconcentrado, la naturaleza jurídica conferida no le resuelve la potestad	

		propia para poder llegar a instituciones más allá del Gobierno Central. 4.22 En el transitorio I se dice que será el Poder Ejecutivo el que en un plazo de seis meses deberá concretar el traslado de los recursos de bienes y personal de la actual Agencia ubicada en el MJP a la nueva Agencia que se establecerá en el MICITT, no obstante; el Poder Ejecutivo está compuesto por varias instituciones, por lo que se recomienda indicar específicamente la o las instituciones del Ejecutivo que tendrán a cargo lo estipulado en dicho transitorio. 4.23 En el transitorio IV se considera que el periodo de adecuación al funcionamiento y lo dispuesto en la ley debe ser mayor a los doce meses; no obstante, considerando que en el transitorio V se le da a la Agencia un plazo de seis meses para crear el Reglamento a la Ley y esto toma parte del tiempo asignado al resto de la institucionalidad para adaptarse a lo estipulado, considerándose las designaciones internas de recurso humano, normativo y de infraestructura para asumir lo dispuesto, se recomienda ampliar y valorar los tiempos transitorios a partir de la realidad y posibilidad. III.- Conclusiones y Recomendaciones 1. Desde el punto de vista de la conformación estructural del sector público costarricense, el proyecto de ley busca modificar la conformación de la institucionalidad pública, por cuanto su propósito es darle un marco competencial, estructura administrativa y recursos a la Agencia de Protección de Datos Personales (anteriormente Agencia de Protección de Datos de los Habitantes (PRODHAB), modificando su adscripción de órgano desconcentrado del Ministerio de Justicia y Paz al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, manteniendo la desconcentración máxima y dotada de independencia operativa, técnica, administrativa, presupuestaria y funcional. 2. La propuesta del proyecto de ley, presenta en su gran mayoría en la redacción, elementos y contenidos propios de protocolos de actuación y que no necesariamente debe incluirse en un texto de ley, por lo que se recomienda valorar la redacción, intencionalidad de lo que se quiere plantear en el documento y los aspectos propios que corresponden a eventuales lineamientos, protocolos o guías que puedan surgir a raíz de la ley y no contenerse en la ley misma. Asimismo, la propuesta del proyecto de ley reúne elementos que actualmente están contenidos en la Ley de Protección de la Persona frente al tratamiento de sus datos personales Ley N°8968 y su reglamento, siendo así que se identificaran redacciones propias y ampliaciones de temas que corresponden a una ley y otras que pueden ser parte de un reglamento que operacionalice lo indicado en este marco normativo. 3. Se recomienda analizar rigurosamente los enunciados sobre el nombramiento de la persona Directora y su adjunto, así como su nomenclatura en cuanto a organización, la asignación presupuestaria que	

		se desea asignar al órgano desconcentrado y otras pautas estructurales con respecto a la existencia de la figura del Oficial de Protección de Datos y su relación con la administración activa propuesta en el texto, con base en principios de oportunidad, sostenibilidad, viabilidad y racionalidad propios de la Administración Pública. 4. Se recomienda valorar el tipo de naturaleza jurídica que se le estaría otorgando a este órgano, a efecto de que pueda desempeñar su trabajo con independencia técnica, dado que al parecer a nivel competencial y potestades que se le están otorgando presenta muchas limitaciones para su puesta en marcha y funcionalidad, ante el jerarca ministerial y otros órganos del Estado costarricense. 5. Mideplan considera, que diversos artículos planteados en esta propuesta de ley, se podrían mantener a nivel reglamentario o bien, ser formalizados mediante un protocolo del tema en cuestión.	
AL-CPECTE-C-0440-2022	Cámara de Incomunicación y Tecnología	Hace una serie de observaciones al proyecto de ley a lo largo del articulado.	17 de noviembre del 2022
CPNCR-DE-193-2022	Colegio de Nutricionistas	Este indica que el texto sustitutivo no varía el fondo del proyecto original y por ello este Colegio mantiene el mismo criterio expresado anteriormente referente al proyecto original.	28 de noviembre del 2022

III. Criterio de Servicios Técnicos:

El cuerpo del proyecto de ley está compuesto por un total de 83 artículos y seis disposiciones transitorias, el cual pretende derogar la *"Ley de protección de la persona frente al tratamiento de sus datos personales"*[1] y la vez, actualizar el marco regulatorio a los más altos estándares en la materia.

IV. Consideraciones de fondo:

En atención a la aprobación de un texto sustitutivo por la Comisión Permanente Especial de Ciencia, Tecnología y Educación, en la sesión ordinaria N°16, del 10 de noviembre de 2022, producto de la aprobación, se hace imperioso realizar un análisis de conexidad de la presente propuesta de ley, a efecto de verificar el cumplimiento del principio de conexidad.

Análisis del principio de conexidad en la propuesta legal

El principio de conexidad en el ámbito legislativo se ha conceptualizado así: *"las modificaciones que se introducen a un proyecto de reforma constitucional, ley o*

[1] La cual está compuesta por 34 artículos y tres disposiciones transitorias.

acuerdo, deben ser conformes con la finalidad o propósito original de la iniciativa y guardar relación con ella."[2]

Este principio de conexidad, la Sala Constitucional lo ha desarrollado en relación con los principios democrático, derecho de iniciativa y el derecho de enmienda; donde determina el lineamiento esencial de este, al indicar que:

> *"Emanan del principio democrático tanto el derecho de iniciativa, regulado en la Constitución, como el derecho de enmienda, del cual se ocupa el Reglamento Legislativo al tratar las llamadas mociones de fondo y de forma. Ambos se originan en ese principio y en su virtud constructiva. El primero implica participación, porque es el medio legítimo de impulsar el procedimiento legislativo para la producción de una ley que recoja los puntos de vista de quien la propone. El derecho de enmienda también es un medio de participar en el proceso de formación de la ley, que hace posible influir en el contenido definitivo de ésta. Ambos derechos están necesariamente relacionados y han de ser observados durante el proceso formativo de la ley, pero ninguno de ellos puede tiranizar al otro (por regla general). Así, por ejemplo, no puede aprovecharse la enmienda para excluir de raíz la materia a la que el proyecto se refiere bajo la particular concepción de su proponente legítimo (ya fuera que se intente o no usurpar las ventajas de un proceso ya avanzado). Pero tampoco puede pretenderse que la iniciativa impone a la Asamblea el limitado deber de aprobar el proyecto o rechazarlo, sin posibilidad de ahormar con arreglo a los diversos puntos de vista de los diputados (...). Es aproximadamente en este sentido que se suele decir que el texto formulado con la iniciativa fija el marco para el ejercicio del derecho de enmienda.*
>
> *(…)*
>
> *Como ha señalado este Tribunal en varias decisiones previas, la garantía que proporciona el principio de conexidad para la protección tanto del derecho de iniciativa, como del derecho de enmienda, en el marco del procedimiento legislativo, atiende esencialmente, a la materia sobre la que versa el proyecto formulado originalmente. Es decir, lo que se pretende con la protección que otorga ese principio no es impedir u obstruir el ejercicio de lo que la Sala ha denominado 'función política transaccional' que se refiere a la posibilidad que tienen las y los diputados de ir ajustando con sus opiniones, dentro del marco que fija la iniciativa, el proyecto originalmente propuesto*".[3]

El principio de conexidad atiende esencialmente a la materia sobre la que versa el proyecto formulado originalmente, al existir una unidad de materia con el texto original. El texto base de la iniciativa de ley, puede sufrir modificaciones –texto transado- siempre que mantenga su unidad lógica y su propia identidad, sin que se

---

[2] **Departamento de Servicios Técnicos**. Oficio N°AL-DEST-CJU-087-2015 de 17 de agosto de 2015. CONSULTA sobre "Conexidad de moción 137 que introdujo modificaciones al inciso a) del artículo 18 de la Ley N°9028, Ley general para el control de Tabaco y sus efectos nocivos, en relación con el contenido del texto del expediente N°19.407, Ley para mejorar la lucha contra el contrabando".

[3] **Sala Constitucional.** Voto N°3441-2004.

altere su materia esencial. Se requiere que el texto sustitutivo mantenga una conexión necesaria y razonable con el texto original.[4] Es decir, el *"balance que debe imperar entre los derechos de iniciativa y enmienda de los legisladores y los límites que a ellos imponen los principios constitucionales de conexidad y democrático",* donde se determina la posibilidad de modificar el texto, siempre y cuando conserve su objeto y sentido original.[5]

De lo anterior, podemos concluir que el principio de conexidad está estrechamente ligado al respeto del hilo conductor del texto base original del proyecto de ley, el cual no puede ser dejado de lado.

En relación con la función política transaccional, que opera a lo interno de los órganos legislativos, específicamente en la discusión del proyecto de ley –texto base-; las enmiendas introducidas en la iniciativa puede ser operada mediante una moción de Texto Sustitutivo[6], -como sucedió en la iniciativa en estudio- donde las modificaciones al texto del proyecto de ley obedecen a los aportes de instituciones públicas, de organismos especializados del sector privado, cámaras empresariales como la Cámara de Tecnologías de Información y Comunicación, y órganos internacionales, como la Asociación Latinoamericana de Internet, Access Now y

---

[4] En este sentido, la Sala Constitucional señaló: *"… la conexidad se dirige, entonces, a lograr que se respete el derecho de iniciativa de conformidad con el cual se establece el hilo conductor básico (la raíz) que ha servido de ratio o motivo para el proyecto original y que, por eso mismo, no puede ser dejado de lado, sea a través de cambios en la finalidad del proyecto, o bien, por la inclusión de meras disposiciones aisladas que regulan temas cualitativamente diferentes".* (Voto N°3441-2004).

[5] *"**V.- Sobre los alcances del principio de conexidad.** En la sentencia No. 2010-16335 de las 15:50 hrs. de 29 de septiembre de 2010 reiteró la Sala anteriores decisiones suyas sobre el balance que debe imperar entre los derechos de iniciativa y enmienda de los legisladores y los límites que a ellos imponen los principios constitucionales de conexidad y democrático, en los términos que siguen: "…el derecho de enmienda deriva del principio democrático y está regulado expresamente por el Reglamento de la Asamblea Legislativa. A través de él, los diputados participan en el proceso de formación de la ley, de manera que pueden influir en el contenido definitivo de ésta a través de la presentación de mociones tendentes a modificar el contenido del proyecto original. De conformidad con la jurisprudencia de este Tribunal, este derecho debe ser observado durante todo el proceso de formación de la ley y constituye "parámetro de constitucionalidad", de manera que una violación a su núcleo básico provoca la inconstitucionalidad de la norma que se aprueba. Este derecho se relaciona íntimamente con el derecho de iniciativa, también de observancia obligatoria durante el procedimiento de aprobación de una ley. Este último supone participación, porque es el medio legítimo de impulsar el procedimiento legislativo para la producción de una ley que recoja los puntos de vista de quien la propone. El objeto del derecho de iniciativa es fundamental, porque sirve de marco referencial durante la tramitación del procedimiento y se convierte en un límite intrínseco para la presentación de enmiendas. En este sentido, la Sala ha insistido en que existe un marco dentro del cual la Asamblea Legislativa puede realizar lo que se denomina "función política transaccional", para la cual tiene, naturalmente, mayor disposición y para la cual la Constitución la estructura (a partir del artículo 105). Por ello, tanto el derecho de iniciativa como el de enmienda deben ser observados durante el proceso de formación de la ley, pero ninguno puede prevalecer sobre el otro. Así, ni el derecho de enmienda puede utilizarse para convertir el proyecto inicial en uno sustancialmente diferente al presentado originalmente –siendo éste uno de sus límites-, ni el de iniciativa puede prevalecer de manera que la Asamblea -y los diputados en particular- vea limitadas sus potestades de discusión y de ajustar el proyecto según se estime pertinente. Es por ello que se ha dicho que el texto propuesto por medio del derecho de iniciativa original es el que fija el marco general del proyecto y se dentro de éste que deben ponderarse las modificaciones que se pretendan introducir por medio del ejercicio del derecho de enmienda." (ver también las resoluciones #2008-10450 de las 9:00 horas del 23 de junio; #2008-5179 de las 11:00 horas del 4 de abril; #2008-2521 de las 8:31 horas del 22 de febrero, las tres de 2008; #2007-17104 de las 9:36 horas del 23 de noviembre de 2007; y la #3513-94 de las 8:57 horas del 15 de julio de 1994, anteriormente citada).*
En suma, puede modificarse o complementarse un proyecto de ley, en tanto éste conserve su objeto y sentido original. De lo contrario, deberá ocurrirse a una nueva iniciativa y a un nuevo proyecto de ley, que contemple los cambios desligados del primer proyecto, cumpliéndose todos los pasos indispensables del procedimiento parlamentario correspondiente." **Sala Constitucional. Voto Nº 5274-2011 de las 15:19 horas del 27 de abril de 2011.**

[6] Las cuales deben perseguir la búsqueda del hilo conductor básico de la orientación en la misma dirección del proponente, aunque no siempre bajo la misma perspectiva. Como ejemplo, se citan los expedientes legislativos N°17.502 *"Sistema de Banca para el Desarrollo"* -**Sala Constitucional** avaló el texto sustitutivo-, y el N°18.255 "Ley de Profesionalización del Servicio Exterior" –criterio del **Departamento de Servicios Técnicos**. Oficio N°AL-DEST-CJU-100-2015 de 25 de setiembre de 2015 en consulta sobre análisis de conexidad del "borrador" de Texto Sustitutivo de la "Ley de Profesionalización del Servicio Exterior", donde avala texto sustitutivo.

Derechos Digitales, enmiendas que fueron congruentes con ajustar la normativa a los más altos estándares en la materia, específicamente, los del Reglamento General de Protección de Datos Personales de la Unión Europea[7], Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales N°3/2018, de España[8] y los Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos Personales[9].

Para el proyecto de ley en estudio, y para efectos de determinar la conexidad del texto sustitutivo aprobado[10], es necesario analizar si el texto respeta el principio de conexidad con el texto original de la iniciativa -texto base-. Para ello, en el apartado de "Anexos", se puede consultar la tabla comparativa entre el texto base presentado y el texto sustitutivo, donde se destacan las enmiendas realizadas al texto sustitutivo.

De la comparación de la estructura de los textos -inicial y sustitutivo-, podemos determinar que ambos mantienen la misma, compuesta por 83 artículos. La diferencia radica, en la adición de una disposición transitoria en el texto sustitutivo[11]. La estructura es la siguiente:

- Capítulo I Disposiciones generales
- Capítulo II Principios de protección de datos personales
- Capítulo III Derechos del titular
- Capítulo IV Responsable y encargado del tratamiento
- Capítulo V Transferencias internacionales de datos personales
- Capítulo VI Medidas proactivas en el tratamiento de datos personales
- Capítulo VII Disposiciones aplicables a tratamientos concretos
- Capítulo VIII Agencia de Protección de Datos
- Capítulo IX Procedimiento en caso de posible vulneración a la normativa de protección de datos
- Capítulo X Régimen sancionador
- Capítulo XI Derecho de indemnización

---

[7] 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.
[8] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de España, la cual entró en vigor el 7 de diciembre de 2018.
[9] Estándares de Protección de Datos Personales para los Estados Iberoamericanos, del 20 de junio de 2017. Los cuales pueden ser consultado en la siguiente dirección web: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
[10] El cual fue aprobado por la Comisión Permanente Especial de Ciencia, Tecnología y Educación, visible en el acta de la sesión ordinaria N° del 10 de noviembre de 2022.
[11] La Comisión Permanente Especial de Ciencia, Tecnología y Educación, en la sesión ordinaria N°16 del 10 de noviembre de 2022 emitió dictamen afirmativo unánime.

- Transitorios

Comparado el contenido de ambos**,** se evidencia que, en el texto sustitutivo, se realizaron modificaciones tanto de orden formal, como de fondo. Las modificaciones de orden formal refieren a:

- Reformas de varios artículos
- Adición de una nueva disposición transitoria -II-

Las otras modificaciones refieren a temas de fondo, donde en algunos casos se amplía o modifica lo planteado en el texto inicial. Dentro de las reformas de fondo, se destacan:

- Se precisa que los principios y derechos en el texto aplican a los habitantes, independientemente de su nacionalidad, y se modifica *"de la región"* por *"del país"* -artículo 1-
- Se adiciona la definición de *"violación de seguridad de los datos personales"*, se elimina la de *"transferencia de datos"*, y se modifican las definiciones de *"anonimización"*, *"base de datos"*, *"cesión de datos"*, *"consentimiento"*, *"datos biométricos"*, *"datos personales sensibles"*, *"datos relativos a la salud"*, *"encargado"*, *"fuentes de acceso público"*, *"grupo económico"*, *"normas corporativas vinculantes"*, *"tercero"* y *"tratamiento"* -artículo 2-
- Se modifica la frase *"Administración Pública centralizada y descentralizada"* por *"Administración Pública en sentido amplio"* -artículo 3-
- Se eliminan los supuestos de no aplicabilidad de la ley de los incisos c y d -artículo 4-
- Se aclara que, en caso de fallecimiento del titular, los únicos legitimados para ejercer los derechos son los herederos, previa acreditación -artículo 5-
- Se cambia *"grupo empresarial"* por *"grupo económico"* -artículo 6-
- Se reforman las *"excepciones generales al derecho a la protección de datos personales"* -artículo 7-
- Se ajusta la redacción, se establece un plazo de verificación no mayor a 10 días hábiles en el punto a), se adiciona un inciso 6, y se cambia la palabra *"transferencia"* por *"cesión"* -artículo 8-

- Se agregan puntos i y j en el inciso 1, que incluyen *"el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable o del Titular en el ámbito del derecho laboral"* y *"El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos"*, como excepciones. Además, se modifica la redacción de los puntos a y d, y se agregan "*investigación en salud"* y *"pandemias debidamente declaradas por las autoridades de salud competentes",* como excepciones a la prohibición -artículo 10-
- Se adiciona que los registros de condenas podrán estar también bajo el control del Ministerio de Justicia y un inciso 2, que indica que los funcionarios judiciales y abogados podrán realizar tratamiento de datos cuando tengan por objeto tratar la información de sus clientes para el ejercicio de sus funciones, bajo la obligación de secreto profesional -artículo 11-
- Se elimina *"bajo ninguna circunstancia un dato personal sensible podrá ser incorporado en una base de datos de acceso público"* -artículo 12-
- Se sustituye *"el responsable observará"* por *"deberá realizarse conforme a los principios"* y se cambia la redacción del listado de principios -artículo 13-
- Se sustituye "*recogió"* por *"recolectó"* y se agrega un inciso 2 que indica que *"En todos los casos anteriores el Titular tendrá derecho de solicitar rectificación de sus datos personales"* -artículo 14-
- El principio de lealtad se modifica para que indique que *"el tratamiento de los datos personales será legítimo solo cuando se realice con fundamento en alguna de las siguientes bases de legitimación:",* y se adiciona un inciso 2 para indicar que los puntos b, c, f y h del inciso 1 estarán sujetos al cumplimiento de estándares internacionales, principios y criterios de legalidad, proporcionalidad y necesidad -artículo 15-
- Se cambia la palabra *"asistencia"* por "*participación"* -artículo 17-

- Se adiciona que además serán desleales los tratamientos que *"excedan las expectativas razonables del Titular respecto a sus finalidades"* -artículo 18-
- Se sustituye *"las transferencias, nacionales o internacionales"* por *"la existencia de cesiones y/o transferencias internacionales"* y se incluye "las categorías de servicios" -artículo 19-
- Se adiciona que el responsable no podrá tratar los datos personales en su posesión para finalidades análogas o compatibles a aquéllas que motivaron el tratamiento original -artículo 20-
- Se modifica el *"principio de exactitud"* -artículo 22-
- Se modifica el nombre a "principio de responsabilidad proactiva" y se agregan 2 incisos que establecen como mecanismos para que el responsable cumpla con el principio, designar un delegado de protección de datos y llevar el registro de tratamiento de datos, cuando sean requeridos por ley. Además, en el punto b del inciso 3 cambia *"sistemas de administración de riesgos"* por *"mecanismos para el análisis de riesgos"* y agrega *"y en caso de que corresponda, evaluaciones de impacto de datos personales"* -artículo 23-
- Se adiciona al encargado como obligado de establecer las medidas. Se cambia "*garantizar"* por *"mantener"* y *"vulneración"* por *"violación de la seguridad de los datos personales"* -artículo 24-
- Se sustituye *"vulneración"* por *"violación"*
- Se modifica el inciso 4 en el sentido de que el responsable *"deberá presentar actualizaciones periódicas a la Agencia de Protección de Datos Personales sobre el informe inicial, cada vez que se disponga de información nueva o diferente sobre el incidente, hasta la fecha en que la investigación del incidente haya concluido y que el incidente asociado se haya mitigado y resuelto por completo."* -artículo 25-
- Se agrega un inciso 3 que indica *"Los derechos del Titular son irrenunciables. Será nula de pleno derecho toda estipulación en contrario."* -artículo 27-
- Se incluye en el inciso 1, que los derechos *"se ejercerán por medio escrito, y serán comunicados al Responsable en los medios que hubiese puesto a disposición del Titular, por medio del oficial de protección de datos (de haberlo),*

o, en su defecto, en su domicilio social o establecimiento comercial abierto al público". También, se adiciona que *"salvo que otro plazo se estableciera en la Ley, la respuesta a una solicitud de ejercicio de derechos por parte de un afectado deberá comunicarse en un plazo de cinco días hábiles posteriores a su recepción, al medio señalado por el afectado."* -artículo 28-

- Se modifican varios puntos del *"derecho de acceso"* -artículo 29-
- Se modifican varios puntos del "derecho de cancelación o supresión" -artículo 31-

  Se agregan en el inciso b los supuestos de *"publicidad"* y *"prospección comercial"*. Tratándose del inciso 2, se aclara que "*el Responsable del tratamiento deberá responder la solicitud en el plazo máximo de cinco días hábiles"* -artículo 32-
- Se modifican varios puntos del *"derecho a no ser objeto de decisiones automatizadas"* -artículo 33-
- Se elimina que por vía reglamentaria se establezcan los requerimientos, plazos, términos y condiciones en los que los titulares podrán ejercer sus derechos y se sustituye con que será improcedente el ejercicio de los derechos ARCO y portabilidad, en los casos ahí establecidos. Asimismo, se adiciona que cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas, deberán estar expresamente establecidas en la ley. Se sustituye la palabra *"canon"* por *"cargo"* -artículo 36-
- Se modifican las *"obligaciones del responsable del tratamiento"* -artículo 37-
- Se modifica la *"cesión de datos"* -artículo 39-
- Se cambia en el inciso 6 la frase *"una norma reguladora de dichas competencias*" por *"acto administrativo"* -artículo 40-
- Se modifican varios puntos de la *"formalización de la prestación de servicios del encargado",* referentes a las cláusulas que debe incluir el contrato de prestación de servicios. Adicionalmente, se aclara que la formalización de la suscripción del contrato de encargo será responsabilidad del responsable -artículo 41-
- Se complementa la frase *"actividades de tratamiento"* con *"de datos personales"* y se sustituye la palabra *"transfirieron"* y *"transferirán"*, por *"cedieron"* y

"cederán". Adicionalmente, se elimina que en el caso de las transferencias realizadas con base en el artículo 44, apartado 1, inciso d), se tuvieran que incluir en el registro, la documentación de garantías adecuadas -artículo 43-

- Se ajusta la estructura de las *"reglas generales para las transferencias internacionales de datos personales"* -artículo 45-
- Se adiciona que el responsable aplicará, desde el diseño, las medidas preventivas, *"teniendo en cuenta el estado de la técnica, el costo de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entrañe el tratamiento de los datos para los derechos y libertades de los Titulares"* -artículo 47-
- Se incluye a la Asamblea Legislativa como una de las entidades en las que el Responsable deberá designar un oficial de protección de datos y que, en el caso de entidades bancarias y financieras, sujetas a la regulación del SUGEF, se designará de acuerdo a las regulaciones sectoriales que se dicten. Además, se elimina que el responsable deba informar a la Agencia de Protección de Datos en un plazo de diez días naturales y se incluye que *"los Responsables que designen un oficial de protección de datos, sea por mandato legal o de forma voluntaria, deberán poner a disposición del Titular sus datos de contacto en cualquier aviso o política de privacidad de la que disponga".* Entre otros ajustes, se incluye que *"el oficial de protección de datos personales estará obligado por el secreto profesional y el deber de confidencialidad en lo que respecta al desempeño de sus funciones"* -artículo 48-
- Se modifican los dos plazos, uno de dos meses y otro de un mes, por cinco días hábiles -artículo 49-
- Se incluye a al encargado, junto con el responsable, como sujeto que podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, contribuir a la correcta aplicación de la Ley y establecer procedimientos de resolución de conflictos. Asimismo, se aclara que los mecanismos de autorregulación mencionados en el inciso 3, serán *"los elaborados por las asociaciones y otras organizaciones, nacionales o internacionales, de alcance general o sectoriales"* -artículo 50-

- Se agrega como supuesto para la evaluación de impacto, los datos relativos a condenas e infracciones penales, en el inciso 4 se modifica la palabra *"podrá"* por *"deberá"*, y se elimina el inciso 6, que indicaba que *"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"*. Por último, se sustituye la frase *"autoridad de control"* por *"Agencia de Protección de Datos"* -artículo 51-
- Se modifica el inciso 8, indicando que *"se prohíbe el uso de sistemas de identificación biométrica en tiempo real en espacios públicos a través de cámaras o sistemas de video vigilancia que tengan por finalidad la identificación indiscriminada o masiva de las personas"* -artículo 52-
- Se aclara que además de los trabajadores del sector público, incluye a los trabajadores del sector privado, y se agregan las salas de lactancia dentro de los supuestos en los que no se admite la instalación de sistemas de grabación de sonidos ni de video vigilancia -artículo 53-
- Se aclara que incluye a los trabajadores del sector privado, no sólo los del sector público -artículo 54-
- Se modifica la totalidad del texto de *"datos relativos al comportamiento crediticio del sector financiero y no financiero"* -artículo 55-
- Se eliminan los puntos b y e del inciso 1, se agrega en el punto iv) que la designación de un representante legal en el país si el promotor de un ensayo clínico no está establecido en el territorio nacional, será *"para que responda por el cumplimiento de las obligaciones derivadas de esta Ley"*, y se sustituye la referencia a *"legislación"* en el inciso e, por *"Ley 9234 Ley Reguladora de Investigación Biomédica"* -artículo 56-
- Se ajustan varios puntos de las "*disposiciones generales".* Los principales son, que se indica que la Agencia de Protección de Datos *"es la autoridad nacional de control encargada de la regulación y protección de los datos personales de los habitantes de la República"* y se modifica la frase *"será un órgano adscrito al MICITT"* por *"será un órgano desconcentrado del MICITT".* Adicionalmente, se

aclara que no podrán *"impugnarse las resoluciones ante el MICITT ni ser avocadas sus competencias por este"* -artículo 61-

- Se aclara que *"la denominación salario base utilizada en esta Ley debe entenderse como la contenida en el artículo 2 de la Ley No. 7337 de 5 de mayo de 1993",* y que no se aceptarán donaciones de empresas que se dediquen a comercialización de datos, *"sean nacionales o internacionales"*. Además, se agrega en el punto b del inciso 1 la frase *"en los términos que establezca el reglamento a esta ley"* -artículo 62-
- Se agregan 2 funciones a la Agencia de Protección de Datos, se modifica el inciso f y se sustituye en el inciso c *"Asesorar"* por *"Emitir criterio"* -artículo 63-
- Se adiciona un inciso, indicando que, para llevar a cabo funciones de investigación, la Agencia podrá *"dictar y ejecutar medidas cautelares en sede administrativa para garantizar la protección de los datos personales de los habitantes".* También, se hace referencia a que la Agencia podrá actuar sin comprobación previa de indicios, cuando se trate de auditorías preventivas -artículo 64-
- Se incluyen los impedimentos para ser nombrado Director y/o Adjunto, así como que cuando cesen de su cargo por incapacidad esta debe ser por 6 meses y cuando sea por condena firme de delito doloso, podrá ser incluso en grado de tentativa -artículo 65-
- Se cambia la palabra *"comunicación"* por *"cesión"* en el inciso 2 -artículo 70-
- Se aclara que los encargados estarán sujetos al régimen sancionador, *"en el cuanto su responsabilidad no se derive de instrucciones giradas por el Responsable, o del incumplimiento de este a las disposiciones de esta Ley o su reglamento"* -artículo 72-
- Se minimizaron los montos de las sanciones -artículo 73-
- Se elimina el punto n del inciso 1, que establecía como infracción muy grave *"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". También, en el punto p se cambia la palabra "*transferencia"* por *"cesión"* -artículo 74-

- Se aclara que constituye una infracción muy grave, además de los otros derechos, no solo el impedimento o la obstaculización o la no atención reiterada de los derechos de supresión, sino también de cancelación -artículo 75-
- Se ajusta el error en la palabra *"tranferido"* en el inciso c y se sustituye por *"cedido o transferido"* -artículo 76-
- Se modifica el plazo de 12 meses por 6 meses -artículo 77-
- Se ajusta el error en la palabra *"desentralizada"* y se corrige por *"descentralizada"*. Se elimina el inciso 3 que indicaba que la Agencia podía proponer también la iniciación de actuaciones disciplinarias contra los funcionarios implicados cuando existan indicios suficientes para ello y se sustituye por *"los funcionarios públicos que incurran en algunas de las infracciones establecidas en los artículos 74, 75 y 76 y se haya demostrado la culpa o dolo en su accionar u omisión, serán sancionados con la suspensión de su cargo por hasta noventa días, sin goce de salario, sin perjuicio de otras sanciones previstas en el régimen disciplinario aplicable al funcionario. 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"* -artículo 79-
- Se cambia el plazo de prescripción de 1 año a 3 años para el ejercicio de acciones tendientes a la reparación de los daños sufridos -artículo 81-
- En la disposición transitoria I se sustituye "Agencia de Protección de los Habitantes" por *"PRODAHB"*.
- Se adiciona la disposición transitoria II para establecer que *"La PRODHAB continuará desarrollando sus funciones hasta que estas puedan ser asumidas de forma coordinada por la Agencia de Protección de Datos Personales creada en esta Ley, una vez que al menos su dirección haya sido designada y cuente con capacidad operativa para funcionar, lo que determinará la dirección mediante resolución que deberá ser publicada en el Diario La Gaceta y comunicada al público en general. Dicha transición deberá completarse en un*

periodo máximo de un año a partir de la entrada en vigor de esta Ley. Todos los procedimientos administrativos que estuvieran en trámite ante PRODHAB serán trasladados a la Agencia de Protección de Datos Personales a partir de que esta entre en funcionamiento, y serán continuados en el estado que estuvieren y hasta su efectiva finalización".

- En la disposición transitoria III, se sustituye *"Agencia de Protección de los Habitantes"* por *"PRODHAB"*.

- En la disposición transitoria IV, se adiciona que además de adecuar su funcionamiento, quienes ostenten condición de responsables y encargados, deberán adecuar el tratamiento de datos personales a las disposiciones de la Ley.

La exposición de motivos enmarca el objetivo del proyecto de ley, al expresar que:

> *"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."*

De manera que las enmiendas realizadas se enmarcan en lo señalado en la exposición de motivos, referente a realizar una reforma legal integral al marco regulatorio en la materia y a su vez, derogar *la "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales".* De esta manera, con la propia explicación de la iniciativa se identifica que el texto sustitutivo obedece a modificar la propuesta del texto inicial, donde se plantean aspectos necesarios que se circunscriben al mismo eje temático que regula el texto inicial.

Es oportuno precisar que las enmiendas realizadas al texto sustitutivo obedecen al estudio del órgano legislativo, con la recepción de opiniones en la materia producto de las consultas por escrito realizadas a las institucionales, con el fin de añadir modificaciones al proyecto para que amplíe o fortalezca los objetivos de la propuesta supracitados.

En consideración con las enmiendas descritas anteriormente, es importante destacar que las enmiendas planteadas en la propuesta de texto sustitutivo mantienen una conexión necesaria y razonable con el texto original. Es decir, las modificaciones guardan un hilo conductor básico, con la unidad lógica y propia de identidad con el texto original -el cual consiste en derogar *la "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales" y realizar una reforma legal integral al marco regulatorio en la materia*-, al ser un objetivo tan amplio, no se altera el contenido de lo propuesta en la exposición de motivos; es decir, se mantiene la naturaleza de ampliar sustancialmente las herramientas necesarias para otorgar mayores derechos y garantías en materia de protección de datos personales, de acuerdo con los estándares internacionales. De forma que esta asesoría considera que el texto sustitutivo en análisis guarda el respeto del principio de conexidad con el texto original.

En este sentido, por la naturaleza de las enmiendas introducidas en el texto sustitutivo, es fundamental el resguardo del principio de publicidad. Es decir, en este caso concreto, se requiere la necesaria publicidad del texto sustitutivo, a efecto de no vulnerar la garantía de la participación ciudadana.

Estándares internacionales base del proyecto

En la exposición de motivos del proyecto se aprecia que el texto normativo tiene una marcada influencia de los más importantes estándares internacionales: el Reglamento (UE) 2060/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD)[12], el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de Estrasburgo del 28 de enero de 1981, y sus Protocolos (Convenio 108), 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, y las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980).

Debido a lo anterior, esta asesoría considera importante presentar a continuación a las y los Diputados, una síntesis de lo más relevante que han desarrollado estos marcos internacionales en la materia, y que ahora se pretenden incorporar en el ordenamiento jurídico costarricense mediante este proyecto de ley.

---

[12] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Reglamento (UE) 2060/679 del Parlamento Europeo y del Consejo

El RGPD desarrolla un derecho uniforme de la protección de datos personales en los países miembros de la Unión Europea (UE), para lo cual establece como prioridades la protección de los datos personales como derecho fundamental, bajo la premisa de permitir al mismo tiempo los flujos transfronterizos de datos personales, no solo entre países miembros de la UE, sino también entre la UE y países no pertenecientes a la Unión y organizaciones internacionales, considerando el Reglamento como necesarias estas transferencias para la expansión del comercio y la cooperación internacional (Considerandos 5 y 101).

Consiente del creciente aumento de la recopilación y automatización en el tratamiento de los datos personales gracias a la evolución tecnológica, el Reglamento ofrece un marco de seguridad jurídica para facilitar la libre circulación de datos personales, garantizando al mismo tiempo un elevado nivel de protección a sus ciudadanos, ya que entiende el Reglamento, además que dicha protección es necesaria para asegurar otros derechos como la libertad, seguridad, justicia, progreso económico y social, así como al bienestar de las personas físicas.

Aunado a lo anterior, el RGPD reconoce el respeto de todos los derechos fundamentales, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística (Considerando 4).

El Reglamento de igual forma establece las pautas principales para el tratamiento de datos personales a través de los siguientes siete principios: licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, responsabilidad proactiva (Art. 5). Adicional, el RGPD plantea varias bases de licitud del tratamiento además del consentimiento informado.

En consecuencia y a causa de los estándares impuestos por el RGPD en el tratamiento de datos personales, las corporaciones multinacionales, en especial las grandes tecnológicas, han decidido observar el cumplimiento del Reglamento para garantizar de forma global la máxima protección de sus usuarios, lo cual se puede entender gracias al tamaño del mercado de la UE, los estándares estrictos establecidos en el Reglamento y la capacidad reguladora, este fenómeno de adaptación de la regulación europea al resto del mundo, se ha conocido como el efecto Bruselas[13].

El RGPD vino a marcar un hito en la materia desde su publicación en el año 2016, por tal razón, varios países en la región han decidido actualizar su legislación o desarrollar nuevas leyes en Protección de datos, adoptando los principios y

[13] https://es.wikipedia.org/wiki/Efecto_Bruselas

derechos expresados en el Reglamento, tal es el caso de Brasil, Ecuador, Paraguay y Panamá, que cuentan con nuevos marcos legales promulgados después del año 2016, y los cuales siguen los lineamientos del RGPD. En el caso de Argentina y Chile estos discuten proyectos para actualizar su legislación, Argentina para reformar su Ley N.°25.326, del año 2000, y los diputados y diputadas de Chile discuten el proyecto de ley que busca reemplazar la Ley N.°19.628, sobre Protección a la Vida Privada y Protección de Datos de Carácter Personal.

El Convenio 108

El Convenio 108[14] es firmado en Estrasburgo Francia el 28 de enero de 1981, y ha sido la base de las leyes internacionales de protección de datos de más de 40 países europeos[15], fue influenciado entre otros, por las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980, y nace del interés de los países miembros de la UE por ampliar la protección de los derechos y las libertades de sus ciudadanos, especialmente el derecho a la vida privada y la libre circulación de información entre los países, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.

Si bien en un inicio su adhesión fue exclusiva para países miembros de la UE, fue hasta el año 2013, que se permite la adhesión de países no miembros de la Unión Europea, siendo Uruguay el primer país no europeo signatario del Convenio. En Latinoamérica, además de Uruguay, México y Argentina son partes del Convenio.

Debido a las nuevas amenazas a la vida privada derivadas del uso de nuevas tecnologías, el Convenio se ha modernizado en el año 2018, bajo el nombre Convenio 108, esta actualización está disponible para adhesión de países a partir de junio del mismo año y en días recientes Argentina ha sido el país número 33, en firmar el Convenio 108.

Para entender la importancia del Convenio para los intereses de Costa Rica, es de tal relevancia a nivel global que el 7 de mayo de 2021, el Instituto Interamericano de Derechos Humanos (IIDH) obtuvo por unanimidad la condición de Observador, lo que evidencia la seguridad jurídica en materia de protección de datos que los países parte proyectan a los demás países, organizaciones o a las personas.

En el año 2018, se celebró en el país el Encuentro Iberoamericano de Protección de Datos concluyó con éxito, en el cual Francisco Peiró, representante de la Delegación de la Unión Europea en Costa Rica, manifestó su interés en que Costa Rica logre la adecuación al Convenio 108, pues según su criterio “invertir en privacidad genera beneficio y crea nuevas oportunidades de negocio” en referencia

---

[14] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. https://rm.coe.int/16806c1abd

[15] Informe Explicativo de Convenio. https://rm.coe.int/informe-explicativo-de-convenio/1680968479.

a la mejora de flujo de datos, garantías e inversión extranjera que este paso podría concebir para nuestro país[16]. De acuerdo con lo señalado por el Proyecto de Ley aquí analizado, uno de sus principales objetivos es cumplir con los estándares de adecuación del Convenio para lograr su adhesión.

Estándares de Protección de Datos Personales para los Estados Iberoamericanos

Los "Estándares de Protección de Datos de los Estados Iberoamericanos"[17] fueron aprobados y publicados por la Red Iberoamericana de Protección de Datos (RIPD o Red), el 20 de junio de 2017. Entre sus propósitos se encuentra impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región.

Los Estándares ofrecen un conjunto de directrices orientadoras que contribuyan a la emisión de normativa en materia de protección de datos personales en iberoamericana para aquellos países que aún no cuentan con estos marcos legislativos, o que sirvan como referente para la modernización y actualización de las legislaciones existentes.

De manera sucinta y conforme al Artículo 1, sus objetivos principales son: a) establecer un conjunto de principios y derechos de protección de datos personales; b) elevar el nivel de protección de datos personales para responder a las necesidades y exigencias internacionales; c) garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos; d) facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras; e) Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos.

En cuanto a los principios que establecen los Estándares, el artículo 10.1. señala que "En el tratamiento de datos personales, el responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad."

También estipula el texto reglas generales para la relación con el Encargado del tratamiento, para las transferencias de datos personales y establece medidas proactivas en el tratamiento de datos personales.

Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980)

Las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980) (Las Directrices) fueron adoptadas bajo los tres principios que siguen los países de la OCDE: democracia pluralista, respeto de los derechos

[16] Encuentro Iberoamericano de Protección de Datos. https://cutt.ly/bMjxGyo
[17] Estándares de Protección de Datos de los Estados Iberoamericanos. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

humanos y economías de mercado abiertas, se hicieron efectivas el 23 de septiembre de 1980[18].

Las Directrices fueron revisadas en el 2013, el texto revisado modernizó el enfoque de la OCDE y reforzó su integración con otros trabajos sobre cooperación en materia de cumplimiento de la ley de privacidad[19], entre ellos el documento del Marco de Privacidad de la OCDE[20].

Similar a los demás instrumentos internacionales previamente reseñados, las Directrices plantean unos principios en línea donde los demás marcos normativos internacionales: limitación de recogida, calidad de los datos, especificación del propósito, limitación de uso, salvaguardia de la seguridad, transparencia, participación individual y responsabilidad.

La OCDE recomienda a sus países miembros implementar Políticas en materia de privacidad para cumplir con las evaluaciones de cumplimiento, pero en especial recomienda a los países "evitar la elaboración de leyes, políticas y prácticas destinadas a proteger la privacidad y las libertades individuales que pudieran crear obstáculos al flujo transfronterizo de datos personales excediendo los requisitos para tal protección" (Tercera Parte).

De lo anterior, se interpreta que en la actualidad la protección de datos es un asunto global que requiere armonización y reglas de aplicación homogéneas en las diferentes jurisdicciones, con el propósito de ofrecer la máxima protección de los datos personales de cualquier persona independiente de su nacionalidad y además garantizar el flujo de datos personales entre países, dentro de un marco de seguridad jurídica, bajo este prisma, se observa que este Proyecto de Ley N.°23.097, se inspira en los marcos internacionales más robustos en Protección de Datos y respecto a los cuales Costa Rica presenta un rezago importante en materia de cumplimiento y adecuación.

V. Sobre el articulado del texto sustitutivo:

La iniciativa, como se mencionó anteriormente, pretende la aprobación de una nueva legislación que incluya la derogatoria de la ley actual. La propuesta de texto sustitutivo contiene más del doble del articulado del actual texto de la Ley N°8968, y se aparta en su mayoría, del contenido de esta.

Como primer elemento importante a tomar en consideración sobre el texto del proyecto de ley, según se ha indicado tanto en la exposición de motivos, la idea es actualizar la regulación a la luz de los parámetros del Reglamento General de

---

[18] Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980). https://www.oecd.org/sti/ieconomy/15590267.pdf.

[19] OECD work on privacy. https://www.oecd.org/digital/ieconomy/privacy.htm.

[20] THE OECD PRIVACY FRAMEWORK. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Protección de Datos N°679-2016, de la Comisión Europea[21], Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales N°3/2018, de España[22] y los Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos Personales[23].

De esta manera, a la luz de las observaciones enviadas por distintos sectores y entidades del país consultadas, el texto sustitutivo incorpora muchas de ellas. Para estos efectos, se presenta un listado de los temas del articulado y las modificaciones introducidas de mayor relevancia, con comentarios.

Disposiciones generales

En el Capítulo I Disposiciones generales se modifican:

- Objetivo -artículo 1-
- Definiciones[24] -artículo 2-
- Ámbito de aplicación subjetivo -artículo 3-
- Ámbito de aplicación objetivo -artículo 4-
- Datos de personas fallecidas -artículo 5-
- Ámbito de aplicación territorial -artículo 6-
- Excepciones generales al derecho a la protección de datos personales -artículo 7-
- Tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y cesiones interinstitucionales de datos en el sector público -artículo 8-
- Tratamiento de datos personales sensibles -artículo 10-
- Tratamiento de datos personales relativos a condenas e infracciones

[21] 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.
[22] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de España, la cual entró en vigor el 7 de diciembre de 2018.
[23] Estándares de Protección de Datos Personales para los Estados Iberoamericanos, del 20 de junio de 2017. Los cuales pueden ser consultado en la siguiente dirección web: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
[24] Específicamente a: Anonimización, Base de datos, Cesión de datos, Consentimiento, Datos Biométricos, Datos genéticos, Datos personales, Datos personales sensibles, Datos relativos a la salud, Encargado, Exportador, Fuentes de acceso público, Grupo económico, Elaboración de perfiles, Normas corporativas vinculantes, Responsable, Seudoanonimización, Sistema de identificación biométrica, Tercero, Titular, Tratamiento, y Violación de la seguridad de los datos personales.

penales -artículo 11-

- Tratamiento de datos personales sensibles obtenidos de fuentes de acceso público -artículo 12-

El artículo 1, referido al objetivo de la ley, aclara que los principios y derechos de protección de datos personales son aplicables a los habitantes, independientemente de su nacionalidad y que la finalidad de facilitar el flujo internacional de datos es coadyuvar el crecimiento económico del país, no de la región; modificaciones que fueron introducidas en contraste con el texto original, en virtud de los comentarios de UCCAEP.

El artículo 2, establece las definiciones. Las siguientes fueron objeto de modificaciones significativas, en aras de precisar su concepto:

Anonimización: Se agrega que la aplicación de medidas para impedir la identificación o reidentificación de una persona física, no debe ser solo sin esfuerzos desproporcionados, sino sin plazos de esta misma naturaleza. Adicionalmente, se agrega que se tendrán en cuenta para estos efectos "*factores como los costos y el tiempo necesario para la identificación o reidentificación de la persona a la luz de la tecnología disponible en el momento del tratamiento*."

Base de datos: Distinto al texto original, se señala que la base de datos será tal, *"independientemente de que los datos se encuentren respaldados en soportes físicos o electrónicos",* por criterio de UCCAEP.[25]

Cesión de datos: Se amplían los sujetos de la definición, al establecer que la cesión de datos también se dará cuando la revelación de estos sea realizada a una entidad u organización distinta al titular, por recomendación de UCCAEP.[26]

Consentimiento: Se mejora indudablemente la aplicación práctica del concepto, al incluir que dicha manifestación de voluntad podrá ser proveniente del representante del titular de los datos.

Datos biométricos: Se incluye al final del concepto la frase *"entre otros"*, con la intención de ejemplificar que dicha definición no se limita únicamente a datos dactiloscópicos o imágenes faciales. Además, se eliminan los datos conductuales, ya que el comportamiento no identifica inequívocamente al titular y se mantiene en constante cambio, como lo indicó la Asociación Latinoamericana de Internet.[27]

Datos personales sensibles: El texto original incluye como criterio para determinar un dato personal sensible aquellos *"cuya utilización indebida puedan dar origen a*

[25] **UCCAEP**. Oficio N° DE-086-22 de 30 de agosto de 2022.
[26] Ibíd.
[27] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022, suscrito por la señora Sissi Maribel de la Peña Mendoza, directora para México y Centroamérica.

discriminación o conlleve un riesgo grave para éste". Esta frase se elimina en el texto sustitutivo, en atención a los comentarios de la Asociación Latinoamericana de Internet, en virtud de que ello requiere de un esfuerzo interpretativo que puede distorsionar la posibilidad de realizar tratamientos legítimos y genera una innecesaria amplitud.[28] Asimismo, en el marco de los comentarios de la misma entidad, los de la Corte Suprema de Justicia[29], y los de CAMTIC[30], se elimina el carácter enunciativo del artículo, para generar mayor seguridad jurídica y eliminar el margen de interpretación.

Datos relativos a la salud: En atención a los comentarios del Colegio de Optometristas[31] y el Colegio de Farmacéuticos[32], se incluye posterior a "*incluida la prestación de servicios de atención sanitaria"*, la frase *"en el ámbito público o privado"*, para mayor seguridad en cuanto a los alcances del concepto.

Fuentes de acceso público: Siguiendo los comentarios de la Asociación Latinoamericana de Internet, se elimina la prohibición presente en el texto original, de existir solo cuando una ley les haya dado ese carácter o sea necesario para cumplir los fines previstos en esa ley. Lo anterior, argumentado con base en el carácter restrictivo de esta limitación[33], lo cual fue, además, replicado por la Corte Suprema de Justicia, indicando que el hecho de que sus bases de datos deban seguir este criterio, afectaría su operatividad[34]. Por otro lado, motivado por la sugerencia de UCCAEP, se enumeran adicionales supuestos de fuentes de acceso público, como: el diario oficial La Gaceta y el Boletín Judicial; las publicaciones realizadas en medios masivos de comunicación; y, las guías, publicaciones, anuarios, directorios y similares que tengan la finalidad comunicar públicamente la pertenencia de determinadas personas a organizaciones gremiales, asociaciones, colegios profesionales[35]. Lo anterior se complementa en el texto sustitutivo, con la inclusión de la frase *"El funcionamiento de las bases de datos de acceso público respetará los términos de la presente Ley, en especial en cuanto a los principios de legitimación y minimización."*

Grupo económico: Previamente titulado *"grupo empresarial"*, se abandona el concepto *"grupo constituido por una empresa que ejerce el control y sus empresas controladas"*, por la dificultad de comprensión que generaba, de acuerdo con el Ministerio de Economía, Industria y Comercio[36]. En cambio, se sustituye por la

---

[28] Ibíd.
[29] **Corte Suprema de Justicia.** Oficio N°SPP155-2022, suscrito por la señora Silvia Navarro Romanini, secretaria general.
[30] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022, suscrito por el señor Christian Sánchez Alcázar, director ejecutivo.
[31] **Colegio de Optometristas de Costa Rica**. Oficio N°COCR-174-Ago-2022 de 22 de agosto de 2022, suscrito por el doctor Enrique Garita Mora, presidente.
[32] **Colegio de Farmacéuticos de Costa Rica.** Oficio N°JD-0184-08-2022 de 23 de agosto de 2022, suscrito por la doctora Lidiette Fonseca González, presidente.
[33] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.
[34] **Corte Suprema de Justicia.** Oficio N°SPP155-2022. Op.cit.
[35] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[36] **Ministerio de Economía, Industria y Comercio.** Oficio N°MEIC-DM-OF-340-2022 de 9 de agosto de 2022, suscrito por la señora Giannina Córdoba Corrales, jefa de despacho.

definición presente en la Ley 9736, por solicitud de UCCAEP[37].

Tratamiento: Se sustituye el concepto *"transferencia"* por *"cesión"*.

Finalmente, se eliminó la definición de transferencia de datos y se incluyó la de violación de la seguridad de los datos personales.

El artículo 3, regula el *"ámbito de aplicación subjetivo"* de la ley, la cual será aplicable a *"las personas físicas o jurídicas de carácter privado, y a la Administración Pública en sentido amplio, que realicen tratamiento de datos personales en el ejercicio de sus actividades y funciones".* En ese sentido, el texto original hacía referencia a la *"Administración Pública centralizada y descentralizada"*, pero se modificó al texto citado, lo cual, con toda seguridad, engloba la totalidad de la Administración.

El artículo 4, regula el *"ámbito de aplicación objetivo"* de la ley, definiendo que esta 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"*. Por otro lado, según la redacción del texto original, los supuestos de inaplicabilidad de la norma son 4:

> *"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."*

A estos efectos, es oportuno valorar la solicitud expresa de Access Now y Derechos Digitales, quienes desarrollaron que *"los datos anonimizados, los datos de personas fallecidas o los datos que constituyen secreto de estado pueden ser excepciones para, por ejemplo, la obtención del consentimiento del titular, más no para otras*

[37] **UCCAEP**. Oficio N° DE-086-22. Op. cit.

estipulaciones"[38]. Por consiguiente, se modificó la redacción dentro del texto sustitutivo, y se eliminaron los incisos c y d.

El artículo 5, establece las pautas para el ejercicio de los derechos reconocidos por la Ley, sobre los datos de una persona fallecida. A estos efectos, en el texto sustitutivo, se cambió el concepto *"personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos"*, por *"herederos, previa acreditación de su condición"*, como los legitimados para ejercer estos derechos. Lo anterior, fundamentado en las sugerencias de la Asociación Latinoamericana de Internet, pues era un concepto amplio que podía dar lugar a suplantación de identidad y generaba inseguridad jurídica en cuanto a sus alcances.[39]

El artículo 6, introduce la regulación del *"ámbito de aplicación territorial"* para el tratamiento de datos personales, en cuatro supuestos:

> *"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."*

En palabras de CAMTIC, el punto d se debería eliminar, pues impone el derecho local a quien contrata un proveedor de servicios o un encargado de tratamiento en el país. Realmente, únicamente debería estar el encargado sujeto a dicha normativa, no el responsable.[40] De forma congruente con lo establecido por este comentario, se eliminó el punto d del inciso 1) de la redacción del texto sustitutivo, lo cual elimina limitaciones innecesarias a servicios como hosting y procesamiento de datos.

---

[38] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza.
[39] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.
[40] **Cámara de Tecnologías de Información y Comunicación.** (CAMTIC) Oficio de 8 de agosto de 2022. Op. cit.

El artículo 7, establece las *"excepciones generales al derecho a la protección de datos"*, es decir, aquellos casos en los que se puede limitar este derecho. Es oportuno citar la opinión de Access Now y Derechos Digitales, donde citan con base en el texto original, que se debe modificar la redacción del artículo, sustituyendo el primer inciso *"Cualquier ley que tenga como propósito limitar el derecho a la protección de datos personales contendrá, como mínimo, disposiciones relativas a:"*, por *"No se podrá limitar el derecho a la protección de datos personales mediante ley, salvo de manera excepcional, cuando existan razones que justifiquen su necesidad, sean adecuadas y proporcionales en una sociedad democrática, y respeten los derechos y las libertades fundamentales de los Titulares"*. De esta manera, se garantiza una protección más amplia a este derecho, al estar la limitación sujeta a excepcionalidad, que además deberá conjugarse con ciertas disposiciones mínimas enlistadas en el artículo.[41]

Por otro lado, bajo las mismas recomendaciones y para mayor congruencia con los motivos anteriormente citados, se elimina el inciso 2, que disponía que *"las leyes serán las necesarias, adecuadas y proporcionales en una sociedad democrática, y deberán respetar los derechos y las libertades fundamentales de los titulares", y* se sustituye por el inciso 3, cuya redacción se mantiene entre ambos textos.

El artículo 8, introduce los *"tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y cesiones interinstitucionales de datos en el sector público"*. Distinto al texto original, en esta versión se aclara que se refiere al sector público y se sustituye la palabra *"transferencia",* por *"cesión"* a lo largo del texto. Asimismo, en atención a los comentarios de UCCAEP, se incluye que "no deberán ser menores a las garantías y derechos establecidos en esta Ley", las condiciones especiales que pueda imponer esta norma, a la hora de realizar tratamientos de esta naturaleza. En este orden de ideas, se fundamenta que los convenios interinstitucionales deben hacer referencia adicionalmente a "los medios para solicitar el efectivo ejercicio de los derechos del Titular"; cambio que se ve reflejado en el texto sustitutivo.[42]

Por otro lado, en este mismo artículo, se introduce que cuando la cesión deba ser autorizada de previo por la Agencia de Protección de Datos, esta deberá verificar en un plazo no mayor a diez días hábiles, el cumplimiento de las siguientes condiciones:

> *"i) la cesión 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*

[41] [41] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.
[42] **UCCAEP**. Oficio N° DE-086-22. Op. cit.

seguridad, protocolos y demás garantías establecidas en esta Ley, para proteger la integridad, disponibilidad y confidencialidad de los datos."

Se incluye que los convenios institucionales deberán ser comunicados a la Agencia de Protección de Datos y se aclara, en un nuevo inciso 6, que *"no se considerará cesión ni transferencia de datos la remisión de datos personales realizada por un Responsable o Encargado del sector público ante una orden de una autoridad judicial competente en el marco de sus facultades legales, siempre que dicha orden se realice dentro de una investigación o procedimiento específico"*.

El artículo 10, titulado *"tratamiento de datos personales sensibles",* sobrelleva una serie de modificaciones, impulsadas por las sugerencias de distintas entidades:

1) Se adiciona en cuanto al inciso d sobre consentimiento expreso, que este *"podrá derivar de un contrato donde el tratamiento de tales datos sensibles resulta indispensable, siempre que así conste que se haya informado al Titular"*, en virtud de los comentarios de CAMTIC. [43]

2) Por sugerencia del Colegio de Optometristas y el Colegio de Farmacéuticos, se incluyen como excepciones *"la investigación en salud"* y las *"pandemias debidamente declaradas por las autoridades de salud competentes"*. [44]

3) Se incluyen 3 nuevas excepciones a la prohibición del tratamiento de datos sensibles en los incisos i, j, k. Desarrollan:

   "i. El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable o del Titular en el ámbito del derecho laboral, de la seguridad social o ayudas sociales, en la medida en que así lo autorice el marco normativo y establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del Titular", motivado por los comentarios de Access Now y Derechos Digitales.[45]

   "j. El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los Titulares", en razón de las sugerencias de UCCAEP, Access Now y Derechos Digitales.[46]

---

[43] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022. Op. cit.
[44] **Colegio de Optometristas de Costa Rica**. Oficio N°COCR-174-Ago-2022. **Colegio de Farmacéuticos de Costa Rica.** Oficio N°JD-0184-08-2022. Op. cit.
[45] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.
[46] Ibíd.

"k. El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial". Este último a solicitud de la Corte Suprema de Justicia, por las implicaciones que el caso contrario podría tener sobre las bases de datos que operan en la actualidad, y que son de consulta obligada y diaria.[47] Asimismo, la redacción incorporada fue propuesta por Access Now y Derechos Digitales.[48]

Sobre el artículo 11, referente al *"tratamiento de datos personales relativos a condenas e infracciones penales"*, es conveniente hacer referencia a los comentarios de la Corte Suprema de Justicia. Indica que, en el texto original, hacía falta una mención sobre *"cómo tratar este tipo de datos cuando una parte en un proceso penal es funcionario público y los hechos están relacionados con el ejercicio de su cargo; ello en tanto no se puede diferenciar donde la ley no lo hace"*.[49] En relación con este tema, se destacan dos ajustes en el texto sustitutivo: 1. La inclusión del Ministerio de Justicia como sujeto facultado para contar con un registro completo de condenas penales. 2. La aclaratoria, expresada a través de un inciso segundo, de que *"además de los funcionarios judiciales involucrados, los abogados en ejercicio podrán realizar tratamiento de datos personales referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas cuando tengan por objeto tratar la información tratada por sus clientes para el ejercicio de sus funciones, bajo la obligación de secreto profesional".*

La norma originalmente incluía en el artículo 12, la prohibición absoluta de la existencia de datos personales sensibles en bases de datos de acceso público. Dicha disposición, como fue desarrollado en los comentarios de la Asociación Latinoamericana de Internet, era excesiva y podía afectar servicios existentes en la actualidad, con profunda necesidad para la población, como lo sería el Diario Oficial La Gaceta.[50] Afortunadamente, se eliminó del texto sustitutivo.

Capítulo II Principios de protección de datos personales

En el *Capítulo II Principios de protección de datos personales* se modifican:

- Principios aplicables al tratamiento de datos personales -artículo 13-
- Principio de exactitud -artículo 14-
- Principio de legitimación -artículo 15-
- Principio de lealtad -artículo 18-
- Principio de transparencia -artículo 19-
- Principio de finalidad -artículo 20-

[47] **Corte Suprema de Justicia.** Oficio N°SPP155-2022. Op.cit.
[48] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.
[49] **Corte Suprema de Justicia.** Oficio N°SPP155-2022. Op.cit.
[50] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.

- Principio de exactitud -artículo 22-
- Principio de responsabilidad proactiva -artículo 23-
- Principio de seguridad -artículo 24-
- Notificación de violación a la seguridad de los datos personales -artículo 25-

En el Capítulo II, Principios de protección de datos personales se incorporaron principios que son parte del Reglamento General de Protección de Datos Personales (RGPDP). Se desarrollan los siguientes principios: exactitud[51], legitimación[52], lealtad[53], transparencia[54], limitación de la finalidad[55], minimización[56], exactitud[57], responsabilidad[58], seguridad[59] y confidencialidad[60].

Este listado se encuentra en el artículo 13, el cual originalmente establecía que *"en el tratamiento de datos personales, el responsable observará los principios de exactitud, legitimación, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad"*. Con las reformas introducidas al texto, en este caso, producto de los comentarios de UCCAEP, se generalizó la disposición, eliminando que será el responsable quien observará estos principios, sino *"el tratamiento deberá realizarse conforme a los principios"*[61]. Algunos de dichos principios, sufrieron cambios en su denominación, específicamente el de proporcionalidad (ahora minimización), exactitud (ahora calidad) y finalidad (ahora limitación de la finalidad).

El artículo 14, regula el *"principio de exactitud"*. Este principio abarca los supuestos en los que la existencia de datos inexactos no es imputable al responsable, teniendo él la obligación de tomar todas las medidas razonables para que se supriman o rectifiquen. En ese sentido, en la redacción del texto sustitutivo, se tomó en consideración la recomendación de UCCAEP, en virtud del cual se incluyó la siguiente oración, a manera de un inciso 2: *"En todos los casos anteriores el Titular tendrá derecho de solicitar rectificación de sus datos personales"*.[62]

El artículo 15, en la regulación del *"principio de legitimación"*, señala los presupuestos bajo los cuales el tratamiento que se realice será legítimo. Siguiendo la línea del ajuste que se realizó en el texto sustitutivo al artículo 13, se modificó el inciso primero para que, en atención a los comentarios de la misma entidad, se

---

[51] Artículo 14.
[52] Artículo 15.
[53] Artículo 18.
[54] Artículo 19.
[55] Artículo 20.
[56] Artículo 21.
[57] Artículo 22.
[58] Artículo 23.
[59] Artículo 24.
[60] Artículo 26.
[61] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[62] Ibíd.

cambiara *"El tratamiento de los datos personales será legítimo solo cuando se realice con fundamento en alguna de las siguientes bases de legitimación"*, en vez de *"El responsable solo podrá tratar datos personales cuando se presente alguno de los siguientes supuestos"*. Por otro lado, es importante tomar en consideración los comentarios de Access Now y Derechos Digitales, donde señalan sobre el texto original que "*tanto el párrafo 2 como el párrafo 3 del Artículo 15 utilizan una terminología ambigua que puede dar lugar a confusión y abarcan supuestos que están cubiertos en su totalidad por otras disposiciones de la misma ley"*. En ese sentido, se eliminaron ambos párrafos. Además, sugirieron agregar un nuevo párrafo dos, para delimitar los alcances de los incisos b, c, f y h, que indique que estos *"estarán sujetos al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad".* [63]

El artículo 18, regula el *"principio de lealtad"*, estableciendo que "*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 o excedan las expectativas razonables del Titular respecto a sus finalidades"*. Cabe resaltar, que la última frase *"o excedan las expectativas..."*, es producto de las sugerencias de Access Now y Derechos Digitales, quienes argumentaron que también debe considerarse desleal el tratamiento de esta naturaleza, no limitándose a aquellos casos de discriminación injusta o arbitraria.[64]

El artículo 19, referido al *"principio de transparencia*", mantiene en su mayoría el texto original. El único cambio recae en el inciso d, que previamente establecía que el responsable debe, entre otros, proporcionar al titular la información sobre *"Las transferencias, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas"*. En palabras de la Asociación Latinoamericana de Internet, *"Esta obligación resulta complicada en la práctica para el responsable, dado que, en el mundo digital globalizado, y en el cual las transferencias internacionales son innumerables, muchas veces es impracticable brindar el nivel de detalle que requiere el artículo, teniendo en cuenta que los países de destino y los destinatarios pueden variar con frecuencia. Tampoco resultaría beneficioso en términos prácticos para los interesados que los responsables proporcionen listados extensos referidos a las transferencias internacionales. En todo caso, siguiendo la línea del GDPR y otras legislaciones de la región, debería bastar y extenderse la posibilidad de cumplir al informar la existencia de transferencias internacionales o categorías de destinatarios"*.[65] Por lo tanto, se modificó el inciso para en adelante leerse *"d. La existencia de cesiones y/o transferencias internacionales de datos personales, los*

[63] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.
[64] Ibíd.
[65] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.

destinatarios, las categorías de datos y finalidades que motivan la realización de las mismas".

El artículo 20, en la regulación del *"principio de finalidad"*, señala que los tratamientos se limitarán al cumplimiento de finalidades determinadas, explícitas y legítimas. Se recomienda incluir en el texto sustitutivo *"o que no resulten"* antes de "análogas y compatibles", en atención a los comentarios de la Asociación Latinoamericana de Internet, en virtud de que *"pueden existir situaciones donde no necesariamente se debe contar con una nueva base legal, como aquellos casos donde la finalidad es análoga o compatible con la finalidad que motivó el tratamiento, es decir, no existen cambios materiales al tratamiento que justifiquen la carga administrativa para ambas partes de obtener nuevamente un consentimiento. Esto coincide con el contenido de varias regulaciones de la región tendientes a proveer de mayor certeza y efectividad jurídica la evidencia de consentimiento respecto de las modificaciones a finalidades de tratamiento*".[66]

El artículo 22, previamente titulado *"principio de calidad"*, regula el *"principio de exactitud",* que establece el deber del responsable de poner en práctica medidas para mantener exactos, completos y actualizados los datos. Asimismo, fue modificado, con base en las sugerencias de las siguientes entidades:

1. Corte Suprema de Justicia: sugirió se aclarare si el tratamiento ulterior de datos personales con fines archivísticos, de investigación o estadísticos, debe ser siempre anonimizado o no, por poder esto afectar el manejo de sus propias bases de datos, como Nexus PJ. Por lo que en el inciso 4 se incluyó *"De igual forma, se entenderán válidas las excepciones contenidas en leyes especiales en materia de archivo, investigación o estadística".*[67]
2. CAMTIC: solicitó incluir una referencia al interés legítimo del responsable en la conservación de los datos, más allá del tiempo requerido para el cumplimiento de la finalidad requerida.[68] Por lo anterior, se incluyó en el inciso 4 que *"el Responsable podrá conservar los datos más allá del plazo de conservación en cumplimiento de un interés legítimo, para el cumplimiento de la finalidad inicial de su tratamiento y con pleno respeto a los derechos y garantías del Titular*".
3. UCCAEP: por la redacción propuesta, se incluyó al final del inciso 1, que el responsable *"adoptará todas las medidas razonables para que se supriman*

---

[66] Ibíd.
[67] **Corte Suprema de Justicia.** Oficio N°SPP155-2022. Op.cit.
[68] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022. Op. cit.

o rectifiquen sin dilación los datos personales que sean inexactos". Adicionalmente, propuso el cambio de nombre previamente descrito.[69]

El artículo 23, incorpora el *"principio de responsabilidad proactiva"*, que enlista los mecanismos que el responsable podrá adoptar, para cumplir con los principios y obligaciones de la norma. Se modificó la redacción de dos de esos mecanismos, establecidos en los incisos b y g, y se agregaron 2 más, en incisos h e i. Esta redacción fue propuesta por UCCAEP, la cual establece:

1. *"d. Implementar medidas para el análisis de los riesgos asociados al tratamiento de datos personales, y en caso de que corresponda, evaluaciones de impacto de datos personales"*. Previamente establecía únicamente sistemas de administración de riesgos asociados al tratamiento de datos personales.
2. *"g. Establecer procedimientos para recibir y responder dudas y quejas de los Titulares"*, adicionando *"en los plazos establecidos en esta Ley"*.
3. *"h. Llevar el registro de tratamiento de datos personales, cuando corresponda conforme lo establecido en esta Ley".*
4. *"i. Designar un delegado de protección de datos personales cuando sea requerido conforme esta Ley*".[70]

El artículo 24, regula el *"principio de seguridad"*, que establece la importancia de medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos. En el texto original, se establecía esto como deber únicamente del responsable. Sin embargo, en el texto sustitutivo se adiciona al encargado. Asimismo, en el listado de factores que debe tomar en cuenta el responsable a la hora de determinar las medidas, se cambia el del inciso a, eliminando, dentro de la consideración del 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".* Lo anterior en atención a los comentarios de UCCAEP[71]. Por otro lado, también se eliminó el inciso 6.

El artículo 25, referido a las *"notificaciones de violación a la seguridad de los datos personales"*, se ajustó en el sentido de que en el inciso 4, se aclaró que la notificación a la que se hace referencia se debe realizar tanto a los titulares afectados, como a la Agencia de Protección de Datos. Asimismo, se incluyó en el inciso 4 que, si bien el Responsable debe notificar la información que tenga a su

[69] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[70] Ibíd.
[71] Ibíd.

disposición, cuando por la gravedad o naturaleza particular del incidente sea imposible identificar todos los elementos anteriores dentro de las 72 horas, debe *"presentar actualizaciones periódicas a la Agencia de Protección de Datos Personales sobre el informe inicial, cada vez que se disponga de información nueva o diferente sobre el incidente, hasta la fecha en que la investigación del incidente haya concluido y que el incidente asociado se haya mitigado y resuelto por completo*". Por lo tanto, se eliminó que deba *"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"*. La denominación de este artículo se modificó, al cambiarse la palabra *"vulneración"*, por *"violación"*.

Capítulo III Derechos del titular

En el Capítulo III Derechos del titular se modifican:

- Derechos de acceso, rectificación, cancelación, oposición (ARCO) y de portabilidad -artículo 27-
- Disposiciones generales sobre ejercicio de los derechos -artículo 28-
- Derecho de acceso -artículo 29-
- Derecho de cancelación o supresión -artículo 31-
- Derecho de oposición -artículo 32-
- Derecho a no ser objeto de decisiones individuales automatizadas -artículo 33-
- Ejercicio de los derechos ARCO y de portabilidad -artículo 36-

En el artículo 27, sobre los *"derechos de Acceso, Rectificación, Cancelación y Oposición y de portabilidad"*, se adiciona un inciso 3, que establece *"Los derechos del Titular son irrenunciables. Será nula de pleno derecho toda estipulación en contrario"*.

En el artículo 28, se establecen las *"disposiciones generales sobre ejercicio de los derechos",* de manera que se desarrolla cómo deben proceder el responsable, encargado y titular, ante una solicitud de ejercicio de derechos. Al respecto, Access Now y Derechos Digitales indicaron, *"Si bien algunos de los derechos incluidos en la ley establecen un plazo para que el responsable cumpla con el pedido del titular del dato otros, como el derecho de acceso, no lo contienen".*[72] Por lo que se incluyó en el inciso 4 un plazo de cinco días hábiles, en el cual responsable deberá comunicar la respuesta a una solicitud de ejercicio de derechos, salvo que la ley establezca otro plazo.

[72] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.

El artículo 29, regula el *"derecho de acceso"*, que versa sobre el derecho del titular, previa acreditación de su identidad, de recibir en un plazo de 5 días, confirmación sobre si se están tratando sus datos. Con este texto sustitutivo se incluyó la aclaratoria sobre el plazo que opera y la acreditación de la identidad del titular. Se agregó, además, otra información que debe brindar el responsable al titular, como: bases legales que legitiman las finalidades del tratamiento, el derecho a a presentar una reclamación ante la Agencia y la información sobre las transferencias internacionales de datos que se hayan efectuado o se prevean efectuar, incluyendo los países de destino. En el caso de esta última, se incluyó en el inciso d, pues se eliminó el contenido previamente establecido, que hacía referencia al plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo. Asimismo, por sugerencia de UCCAEP, se incluyó la existencia o no de decisiones automatizadas respecto del tratamiento de sus datos personales, incluida la elaboración de perfiles, como información que debe brindar el responsable.[73]

En el artículo 31, se incluye el *"derecho de cancelación o supresión",* cuyo título fue modificado al adicionar *"supresión"* y eliminar la referencia que previamente se hacía al derecho de olvido. Lo anterior, en razón de que, como lo fundamenta la Asociación Latinoamericana de Internet, se trataba de derechos diferentes. En virtud de los mismos comentarios, se eliminó el inciso 2 que versaba sobre la obligación del responsable de informarle a otros responsables la supresión de datos. Esto se tornaría muy arduo y oneroso para el responsable.[74] Asimismo, en el inciso 2.c, se eliminó *"en el ámbito de salud pública"*, para que más bien, se refiriera al interés público en general. Al inciso 1.e se le agregó el supuesto de que los datos se deban suprimir para cumplir con una orden de autoridad competente.

Finalmente, se adicionó un inciso 2.f, el cual exime al responsable del deber de proceder con la cancelación, cuando *"los datos personales deban ser conservados durante los plazos previstos en disposiciones legales o contractuales, entre el Responsable o Encargado del tratamiento y el Titular de los datos"*.

El artículo 32, estipula los supuestos en los que el titular puede oponerse al tratamiento de sus datos personales, conocido como *"derecho de oposición"*. Se incluyen nuevos supuestos, tales como la publicidad y la prospección comercial, así como se impone al responsable un plazo máximo de 5 días hábiles para responder la solicitud.

El artículo 33, incluye el *"derecho a no ser objeto de decisiones individuales automatizadas",* el cual consiste en el derecho a no ser objeto de una decisión basada en el tratamiento automatizado de datos, incluida la elaboración de perfiles. Por medio de una redacción propuesta por la Asociación Latinoamericana de Internet*,* además del criterio de que produzcan efectos jurídicos al titular, se introdujo que afecten sus intereses de forma significativa. Además, en atención a

[73] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[74] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.

los mismos comentarios, en el inciso 3, se insertó como excepción al derecho del titular de recibir una explicación sobre la decisión tomada, *"siempre que no revelen con dicha explicación secretos comerciales"*.[75]

El artículo 36, plantea la forma en la que el titular puede ejercer sus derechos ARCO y de portabilidad e impone al responsable el deber de contar con mecanismos y procedimientos para esos efectos. En relación con el texto anterior, la Asociación Latinoamericana de Internet destacó que el hecho de que se incluyera la regulación por vía reglamentaria de los requerimientos, plazos y condiciones en que el titular puede ejercer sus derechos, provoca incertidumbre para ambas partes.[76] En ese sentido, se eliminó esa disposición del texto. Otra modificación relevante, fue que se eliminó la referencia a que las causales en las que el titular no puede ejercer sus derechos se enlistaban *"de manera enunciativa más no limitativa"*.

Capítulo IV Responsable y encargado del tratamiento

En el Capítulo IV Responsable y encargado del tratamiento se modifican:

- Obligaciones del responsable del tratamiento -artículo 37-
- Cesión de datos -artículo 39-
- Formalización de la prestación de servicios del encargado -artículo 41-

El artículo 37, regula expresamente los deberes del responsable del tratamiento, así como los riesgos que pueden producirse a la hora de adoptar medidas, en distintos supuestos. En el texto sustitutivo, se eliminó el inciso 1, que establecía la obligación del responsable de definir las medidas técnicas y organizativas que implementaría, y la obligación concreta de valorar si procedía una evaluación de impacto. En consecuencia, se incluyó un nuevo inciso 1, acompañado de puntos de las letras a-k. Indican lo siguiente:

> *"1. Los Responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley, sus normas reglamentarias y otras que rijan su actividad:*
>
> *a. Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y sus normas reglamentarias, especialmente los derechos de los Titulares y la materialización de los principios del tratamiento de datos personales;*

[75] Ibíd.
[76] Ibíd.

b. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de protección de datos, especialmente conocer, actualizar, rectificar, suprimir sus datos personales u oponerse al tratamiento de los mismos;

c. Cumplir debidamente con el deber de informar al Titular sobre la finalidad de la recolección y sus derechos;

d. Tratar los datos personales bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e. Implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos, exactos y comprobables;

f. Actualizar los datos personales, rectificar la información cuando sea incorrecta y adoptar medidas necesarias para que la misma se mantenga actualizada;

g. Tramitar debidamente las solicitudes presentadas por el Titular, respondiéndolas de manera completa y oportunamente;

h. Realizar la notificación de violaciones de seguridad en los términos y plazos previstos en esta Ley.

i. Cumplir las instrucciones, órdenes o requerimientos que imparta la Agencia de Protección de Datos Personales.

j. Formalizar mediante la suscripción de un acuerdo, contrato o cualquier otro instrumento jurídico la prestación de servicios entre el Responsable y el Encargado, en entre corresponsables.

k. Verificar que los Encargados, o quienes éstos subcontraten, ofrecen garantías suficientes para realizar el tratamiento de datos personales conforme con los requisitos de la presente Ley y garantice la protección de los derechos del Titular. Dicha verificación debe realizarse con anterioridad a la contratación u realización de otro acto jurídico que lo vincule con el Encargado;

l. Exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y debido tratamiento de la información del Titular;"

Sobre la redacción original del artículo 39, que regula la cesión de datos, la Asociación Latinoamericana de Internet señalo la necesidad de modificarla, por las siguientes razones:

> *"Se sugiere aclarar el término comunicación y cesión, ya que una comunicación de datos podría darse en una relación de responsable-encargado, en donde el consentimiento del titular del dato no es necesario o existen otros casos en los que otras bases legales deberían poder utilizarse. No se explica razonablemente porque el consentimiento se convierte en la única base legal para las comunicaciones a terceros. Además, sería conveniente modificar el inciso 1 para que se haga referencia únicamente a las cesiones de datos y no a las comunicaciones en general, pues las mismas están sujetas a diversos casos."*[77]

Por consiguiente, se eliminó la palabra *"comunicación"* a lo largo del texto. Por otro lado, se adicionó en el inciso 2, la obligación de quienes cedan datos, de *"facilitar al Titular de los datos personales cedidos la siguiente información, dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos:"*. Dicha información, es la siguiente:

> *"a) la identidad y los datos de contacto del Responsable y, en su caso, de su representante;*
>
> *b) los datos de contacto del delegado de protección de datos, en su caso;*
>
> *c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;*
>
> *d) las categorías de datos personales de que se trate;*
>
> *e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;*
>
> *f) en su caso, la intención del Responsable de transferir datos personales a un destinatario en un tercer país.*
>
> *3. Las disposiciones del apartado anterior no serán aplicables cuando y en la medida en que:*
>
> *a) el Titular ya disponga de la información;*
>
> *b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. En tales casos, el Responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del Titular;*

[77] Ibíd.

c) la obtención o la comunicación esté expresamente establecida en una ley, o;

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional emanada en una norma de carácter legal."

El artículo 41 regula la "*formalización de la prestación de servicios del Encargado",* desarrollando que se dará por medio de la suscripción de un contrato de encargo, cuya formalización es deber del responsable. Al respecto, de acuerdo con las recomendaciones de la UCCAEP, se modificaron los incisos 3.d, 3.e, 3.f y 3.k. A los primeros dos, se les agregó una aclaratoria de que cuando el deber del encargado, en relación con las cláusulas del contrato, consista en informar al responsable, deberá hacerlo sin dilación alguna. Sobre el inciso 3.f, se incluyó que el encargado debe *"garantizar que su personal y cualquier persona autorizada por el Encargado para tratar datos personales del Responsable cuenten con obligaciones contractuales o derivadas de una obligación legal que les obliguen a respetar la confidencialidad de los datos personales tratados"*. Finalmente, se añadió al inciso 3.k que, además del deber del encargado de colaborar con el responsable en lo relativo al cumplimiento de la legislación, debe *"facilitar la información necesaria para demostrar el cumplimiento de las obligaciones en el presente artículo, sea en el marco de una auditoría realizada al Responsable, de un procedimiento de fiscalización por una autoridad competente o cuando dicha obligación derive del contrato de encargo*".[78]

Capítulo V, Transferencias internacionales de datos personales

En el *Capítulo V Transferencias internacionales de datos personales* se modifican:

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

El artículo 45 versa sobre las reglas para llevar a cabo transferencias internacionales de datos personales, así como los supuestos en los que son procedentes. Por consiguiente, y de acuerdo con los comentarios de UCCAEP, se ajustó la estructura del artículo, incluyendo subtítulos en cada inciso que resumen su contenido.[79] También, se incluyó en el inciso c la aclaración de que cuando el país destinatario acredite condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado, estas *"no podrán ser menores que las reconocidas en la presente Ley"*. Además, incorpora en el inciso d, para el caso de transferencias fundamentadas en garantías adecuadas del exportador, que el exportador debe acreditar el cumplimiento de derechos exigibles y el acceso a acciones legales efectivas.

[78] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[79] Ibíd.

Por último, se adicionó un inciso 4 que indica *"cuando el Titular de forma libre, voluntaria y por su propia iniciativa, transfiera sus datos a un Responsable situado en una jurisdicción diferente a la del Titular"*.

Capítulo VI, Medidas proactivas en el tratamiento de datos personales

En el *Capítulo VI Medidas proactivas en el tratamiento de datos personales* se modifican:

- Privacidad por diseño y privacidad por defecto -artículo 47-
- Oficial de protección de datos personales -artículo 48-
- Intervención del oficial de protección de datos en caso de reclamación ante la Agencia de Protección de Datos -artículo 49-
- Mecanismos de autorregulación -artículo 50-
- Evaluación de impacto a la protección de datos personales -artículo 51-

El artículo 47, regula el deber del responsable de poner en práctica medidas preventivas, programas, servicios o sistemas que permitan aplicar o se ajusten a los principios, derechos y demás obligaciones en la Ley. En ese sentido, se incluyó en el inciso 1 que *"teniendo en cuenta el estado de la técnica, el costo de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entrañe el tratamiento de los datos para los derechos y libertades de los Titulares"*, el responsable aplicará esas medidas desde el diseño. Dicha sugerencia proviene de los comentarios de UCCAEP.[80]

El artículo 48, establece los supuestos en los que el responsable debe nombrar un oficial de protección de datos personales, al igual que el detalle de sus funciones y desarrollo de sus labores. Incorporando algunos de los comentarios de UCCAEP, se realizaron las siguientes modificaciones:

- Se incluyó a la Asamblea Legislativa como una de las entidades en las que el responsable debe nombrar un oficial.

- Se aclaró que dicho nombramiento en el caso de las entidades bancarias y financieras, sujetas a la regulación de SUGEF, será "*de acuerdo a las regulaciones sectoriales que se dicten"*.

- Se eliminó del inciso 3, el deber del responsable de informar en un plazo de 10 días naturales a la Agencia de Protección de Datos las designaciones, nombramientos y ceses de los oficiales. En cambio, se dispuso que *"los Responsables que designen un oficial de protección de datos, sea por mandato legal o de forma voluntaria, deberán poner a disposición del Titular sus datos de contacto en cualquier aviso o política de privacidad de la que disponga"*.

[80] Ibíd.

- En el inciso 4, se aclaró que, cuando el oficial desempeñe otras funciones, estas no deberán dar lugar a conflicto de intereses.

- Se eliminó en el inciso 4, que la Agencia tuviera que contar con una lista actualizada de los oficiales, accesible por medios electrónicos.

- Se agregó un inciso 10 que establece el secreto profesional y deber de confidencialidad que cubre al oficial.[81]

El artículo 49, regula la *"intervención del oficial de protección de datos en caso de reclamación ante la Agencia de Protección de Datos".* Ambos plazos estipulados en los incisos 1 y 2, de dos meses y un mes respectivamente, se cambiaron a cinco días hábiles. El primero hace referencia al plazo del oficial para comunicar al afectado la decisión que se hubiera adoptado, contados desde la recepción de la reclamación. El segundo se refiere al plazo que tiene el oficial para responder, cuando la Agencia le remita la reclamación.

El artículo 50, establece que el responsable y encargado pueden adherirse a mecanismos de autorregulación vinculantes para promover la aplicación correcta de la Ley y procedimientos de resolución de conflictos entre el responsable y el titular. Previamente, el texto original incluía esta facultad únicamente para el responsable, pero fue modificado tomando como base los comentarios de UCCAEP. Asimismo, en el inciso 3 se adicionó, que las reglas que defina la Agencia en relación con el reconocimiento de los mecanismos de autorregulación son los *"elaborados por las asociaciones y otras organizaciones, nacionales o internacionales, de alcance general o sectoriales"*.[82]

El artículo 51, regula la *"evaluación de impacto a la protección de datos personales"*, la cual se llevará a cabo por parte del responsable, en casos de tratamientos que probablemente entrañen un alto riesgo de afectación a la protección de datos personales. Con el texto sustitutivo y de acuerdo con los comentarios de UCCAEP, se incluyó en el inciso 3.b, como supuesto dentro de los cuales debe realizarse la evaluación, el tratamiento de datos *"relativos a condenas e infracciones penales previstos en esta Ley"*.[83] Además, se eliminó el antiguo inciso 6 y se sustituyó por el contenido del inciso 7, en el cual se cambió la *"autoridad de control"* por la *"Agencia de Protección de Datos"*.

Capítulo VII Disposiciones aplicables a tratamientos concretos

En el *Capítulo VII Disposiciones aplicables a tratamientos concretos* se modifican:

- Tratamiento con fines de videovigilancia -artículo 52-

[81] Ibíd.
[82] Ibíd.
[83] Ibíd.

- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo -artículo 53-
- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral -artículo 54-
- Datos relativos al comportamiento crediticio del sector financiero y no financiero -artículo 55-
- Tratamiento de datos en la investigación en salud -artículo 56-

El artículo 52, establece el *"tratamiento con fines de videovigilancia"*. En cuanto al inciso 8, la Asociación Latinoamericana de Internet, desarrolló: *"Asimismo, el numeral 8 señala que se prohíbe, sin excepción, el uso de sistemas de identificación biométrica en tiempo real en espacios públicos para cualquier finalidad, especialmente policiales o de investigación criminal. En todo caso, se debe considerar este adelanto tecnológico y la aplicabilidad en el beneficio en la agilización de procesos investigativos, especialmente en delitos relacionados con el salvaguardo de la integridad física de las personas, se recomienda analizar la posibilidad de desarrollar y regular los casos en que podría ser aplicable"*.[84]

En consecuencia, se ajustó el inciso 8, eliminando dicha disposición restrictiva. En cambio, se incluyó que *"se prohíbe el uso de sistemas de identificación biométrica en tiempo real en espacios públicos a través de cámaras o sistemas de videovigilancia que tengan por finalidad la identificación indiscriminada o masiva de las personas"*.

El artículo 53, regula el *"derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo"*, indicando en qué supuestos el empleador puede tratar imágenes obtenidas a través de esos sistemas, y en cuáles su instalación no es permitida. En el texto sustitutivo, se cambió la redacción *"trabajadores o los empleados públicos"*, por *"trabajadores del sector público o privado"*, lo cual define con mayor claridad el ámbito de aplicación de esta norma. Asimismo, de acuerdo con los comentarios de UCCAEP, se incluyeron las salas de lactancia como uno de los supuestos en los que no se admite la instalación de estos sistemas.[85]

Al artículo 54, sobre el *"derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral"*, se le realizó el mismo cambio que al artículo pasado, en cuanto se cambió *"trabajadores o empleados públicos"*, por *"trabajadores del sector público o privado"*. Lo anterior, evita que haya un margen de interpretación sobre el ámbito de aplicación de la norma.

El artículo 55, versa sobre los *"datos relativos al comportamiento crediticio del sector financiero y no financiero"*. Previamente estaba titulado *"sistemas y proveedores de información crediticia"*. Su redacción en el texto inicial fue objeto de diversas críticas, por lo que es uno de los pocos artículos que fueron modificados en su totalidad. La

[84] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.
[85] **UCCAEP**. Oficio N° DE-086-22. Op. cit.

redacción anterior, se enfocaba en que los datos relativos al comportamiento crediticio se regían por las normas que dicte SUGEF, permitiendo a las entidades de esta naturaleza acceder a ellos, sin comprometer los derechos y garantías en la Ley. Indudablemente, era necesaria una redacción más amplia que brinde una protección más extensa y clara al derecho de protección de datos personales. En consecuencia, se incluyó la siguiente redacción en el texto sustitutivo:

> *"1. Los datos personales relativos al comportamiento crediticio tratados por el Centro de Información Crediticia (CIC) se regirán por las normas dictadas por la Superintendencia General de Entidades Financieras, 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, respetando las garantías, principios y derechos concedidos en esta Ley. Esto sin perjuicio del tratamiento que sobre datos crediticios puedan hacer otros Responsables del sector no financiero, en los términos indicados en el presente artículo.*
>
> *2. Queda expresamente autorizado el tratamiento de datos personales destinado a informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos datos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial y/o crediticio que permitan evaluar los riesgos de contratación, la conducta comercial y/o la capacidad de pago del Titular. Lo anterior, en los casos en que dichos datos personales sean obtenidos de fuentes de acceso público, y/o procedentes de informaciones facilitadas por el acreedor con base en su interés legítimo prevalente, o en las circunstancias previstas en la presente Ley.*
>
> *3. Cuando se realice una cesión de datos personales para el fin indicado en el párrafo anterior, el acreedor, en calidad de Responsable de los datos, deberá mantener un registro del Titular de los datos cedidos, que podrá ser requerido por la Agencia de Protección de Datos en el marco de una investigación o procedimiento sancionatorio.*
>
> *4. Los datos personales relativos al comportamiento crediticio que sean significativos para evaluar la solvencia económica o financiera podrán tratarse hasta por cuatro años, desde el vencimiento del plazo original de la operación de crédito. El plazo se reduce a dos años cuando el deudor cancele o extinga la obligación, plazo a contar a partir de la fecha en que lo hace, debiendo constar esta información en el informe crediticio.*
>
> *5. Cuando se cancele una obligación incumplida registrada en una base de datos de solvencia, o exista una orden judicial o administrativa que así lo ordene, el acreedor de la obligación deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al Responsable de la base de datos de solvencia. Una vez recibida la comunicación por el Responsable de la base de datos de solvencia, éste dispondrá de un plazo máximo de tres*

días hábiles para proceder a la actualización del dato, asentando su nueva situación en el informe crediticio.

6. Los Responsables de las bases de datos sobre solvencia o insolvencia patrimonial deberán en todo momento velar por realizar valoraciones objetivas de la información, sin que esta pueda prestarse para ningún tipo de discriminación. Dichas condiciones serán supervisadas por la Agencia de Protección de Datos."

El artículo 56, define los criterios por los cuales se rige el tratamiento de datos en la investigación de salud. Con el texto sustitutivo, se eliminaron los incisos b y e, de manera que se protegen los derechos de los titulares de una manera más rigurosa. Al respecto, el Colegio de Profesionales en Informática y Computación, consideró que esos incisos no eran aceptables. Los motivos se exponen a continuación:

El inciso b contenía una autorización excesiva, ya que, faculta los estudios científicos sin consentimiento de los afectados, con base en "situaciones de excepcional relevancia y gravedad para la salud pública". Deja a interpretación del funcionario público la aplicación de la norma. Sobre el inciso e, es de alto riesgo lo dispuesto en el punto iii), que deja abierta la posibilidad de excepcionar los derechos de los titulares, cuando la investigación tenga "otros objetivos importantes de interés público general". Se puede prestar para que cualquier interés particular calce bajo esta definición. En ambos casos, se promovía que se excepcionaran los derechos o garantías del titular para este tipo de tratamiento, por lo que su eliminación era oportuna.

Finalmente, de acuerdo con los comentarios de la misma entidad, para mayor claridad en el inciso g, se hace referencia a que el comité ético, es aquel previsto en la Ley N.°9234, Ley Reguladora de Investigación Biomédica.[86]

Capítulo VIII Agencia de Protección de Datos

En el *Capítulo VIII Agencia de Protección de Datos* se modifican:

- Disposiciones generales - artículo 61-
- Régimen económico presupuestario -artículo 62-
- Funciones -artículo 63-
- Potestades -artículo 64-
- Dirección de la Agencia de Protección de Datos -artículo 65-

El artículo 61, menciona las disposiciones generales relacionadas con la Agencia de Protección de Datos y su estructura. El antiguo inciso 1, pasó a ser el 2, y en su

[86] **Colegio de Profesionales en Informática y Computación.** Oficio AL-014-JD-CPIC-2022 de 11 de agosto de 2022, suscrito por Hilda Isabel Delgado Montes, asesora legal.

lugar, se incluyó que la Agencia *"es la autoridad nacional de control encargada de la regulación y protección de los datos personales de los habitantes de la República"*. Además, en el inciso 3, se adiciona una mención al MICITT, para referirse a que ante este no se pueden impugnar las resoluciones de la Agencia, ni podrá este avocar sus competencias. Dichas modificaciones recogen parte de los cambios propuestos por UCCAEP.[87]

El artículo 62, regula el régimen económico presupuestario de la Agencia, lo cual abarca los componentes del presupuesto y las entidades encargadas de su fiscalización y auditoría. Al inciso a, se le incluyó al final del texto que "*la denominación salario base utilizada en esta Ley debe entenderse como la contenida en el artículo 2 de la Ley No. 7337 de 5 de mayo de 1993"*. Adicionalmente, se aclaró que, sean nacionales o internacionales, no se pueden aceptar donaciones de empresas que se dediquen a la comercialización de datos. Lo anterior, de forma congruente con los comentarios enviados por UCCAEP.[88]

El artículo 63, enlista las funciones de la Agencia de Protección de Datos. Con el nuevo texto, se modifican algunas y se adicionan 2. En cuanto al inciso c, se cambia para que la función consista en *"emitir criterio"*, no *"asesorar"*. El inciso f establecía como función resolver las reclamaciones de los titulares u organismos y llevar a cabo una investigación al respecto. Actualmente, se cambió su contenido por *"Investigar, resolver y sancionar, de oficio o a ante denuncia, cualquier infracción atribuida a una persona física o jurídica, del sector público o privado, e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable"*.

Asimismo, siguiendo la línea de los comentarios de CAMTIC[89] y UCCAEP[90], se incluyeron dos funciones al final del artículo. La primera, se refiere a *"emitir dictámenes no vinculantes a solicitud de interesados, con el objeto de brindar criterios generales sobre el cumplimiento de las obligaciones y ejercicio de derechos contemplados en esta Ley y los reglamentos que la desarrollen"*. El segundo, adiciona "*Gestionar y administrar sus recursos y presupuesto, para lo que podrá aprobar los contratos de obras y servicios, de acuerdo con el ordenamiento jurídico vigente"*.

El artículo 64, establece las potestades de la Agencia, que podrá ejercer para llevar a cabo sus funciones de investigación. Se incluyó una potestad, relativa a que la Agencia pueda dictar medidas cautelares en sede administrativa para garantizar el derecho de protección de datos. Esto, relacionado con los comentarios de UCCAEP.[91] En el último párrafo se incluyó que, en el caso de auditorías preventivas, puede actuar sin comprobación previa de indicios.
El artículo 65, regula la *"dirección de la Agencia de Protección de Datos".* En ese sentido, menciona cómo será el nombramiento de la Dirección y el Adjunto, la

[87] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[88] Ibíd.
[89] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022. Op. cit.
[90] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[91] Ibíd.

duración de este y las formas en las que podrá cesar. Fue modificado en los siguientes términos:

- Se adicionaron las causales de impedimento para ser nombrado como Director y/o Adjunto, las cuales se refieren a que no podrán ser nombrados en estos puestos, quienes sean parientes "hasta tercer grado de consanguinidad o afinidad del presidente de la República, los vicepresidentes, los ministros y viceministros o con vínculo civil por afinidad hasta el mismo grado".

- En el inciso 5.b se aclara que cuando el Director o Adjunto, cesen de su cargo por incapacidad física sobrevenida para el ejercicio de su función, esta deberá ser por un plazo superior a seis meses.

En el inciso 5.c, se adiciona que cuando el Director o Adjunto, cesen de su cargo por condena firme por delito doloso, esto podrá ser incluso en grado de tentativa.

Capítulo X Régimen sancionador

En el *Capítulo X Régimen sancionador* se modifican:

- Sujetos responsables -artículo 72-
- Infracciones -artículo 73-
- Infracciones consideradas muy graves - artículo 74-
- Interrupción de la prescripción de la infracción - artículo 77-
- Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento -artículo 79-

El artículo 72, regula quiénes están sujetos al régimen sancionador establecido en este capítulo. En el texto original, se mencionaban el responsable y el encargado. Sin embargo, con el texto sustitutivo se hace una aclaratoria en cuanto al segundo, indicando que este estará sujeto al régimen sancionador *"en el cuanto su responsabilidad no se derive de instrucciones giradas por el Responsable, o del incumplimiento de este a las disposiciones de esta Ley o su reglamento"*. De esta manera, se sigue lo recomendado por CAMTIC, quien expuso en sus comentarios que no tiene sentido sancionar al encargado por las acciones que este realice amparado en las instrucciones del responsable.[92]

El artículo 73, fija los montos de las sanciones por actos y conductas contrarias a la Ley. Su redacción anterior, generó preocupación de entidades, tales como el Colegio de Optometristas y el Colegio de Farmacéuticos, quienes destacaron que

[92] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022. Op. cit.

los montos eran elevados. Especialmente, fue inquietante la magnitud del volumen de ventas como criterio para determinar la sanción en caso de personas jurídicas, pues tratándose, por ejemplo, de los colegios profesionales, tienen una realidad económica que dista por mucho de empresas de ventas.

Por consiguiente, se ajustaron los montos de las multas en el texto sustitutivo, disminuyéndolas. En adelante, son las siguientes:

> "a. Para las faltas leves, una multa hasta de entre cinco y diez salarios base.
>
> b. Para las faltas graves, una multa de diez a cincuenta salarios base.
>
> c. Para las faltas gravísimas, una multa de cincuenta hasta cien salarios base, y, en caso de personas físicas o jurídicas que cometieran la infracción en el ejercicio de una actividad lucrativa, el monto superior entre cien 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."

De esta manera, se implementa en cambio, el criterio en las faltas gravísimas, de *"personas físicas o jurídicas que cometieran la infracción en el ejercicio de una actividad lucrativa"*, de la mano de una determinación del monto inferior a la expuesta en el texto original. Además, el volumen de ventas se redujo de 4% a 2%.

El artículo 74, define los supuestos en los que se comete una infracción clasificada como muy grave. En comparación con el texto original, se eliminaron en los incisos k y l, la referencia a los artículos 45 y 64, de la ley, respectivamente. Lo anterior, en concordancia con los comentarios de UCCAEP.[93] Asimismo, se eliminó el inciso n, que abarcaba la no facilitación del acceso del personal de la autoridad de protección de datos, a los datos, información o equipos cuando sean requeridos por esta, para el ejercicio de sus poderes de investigación.

El artículo 77, regula la *"interrupción de la prescripción de la infracción"*. Su contenido versa sobre el plazo durante el cual, si el expediente sancionador está paralizado, se interrumpe el plazo de prescripción de la infracción. Dicho plazo, previamente era de doce meses, pero se cambió a seis.

El artículo 79, menciona el *"régimen aplicable a determinadas categorías de responsables o encargados del tratamiento"*. Se eliminó la redacción original del inciso 3, que establecía la facultad de la Agencia de proponer la iniciación de actuaciones disciplinarias contra los funcionarios implicados, cuando existan indicios suficientes para ello. En cambio, se introdujo que *"los funcionarios públicos que incurran en algunas de las infracciones establecidas en los artículos 74, 75 y 76 y se haya demostrado la culpa o dolo en su accionar u omisión, serán sancionados con la suspensión de su cargo por hasta noventa días, sin goce de*

[93] **UCCAEP**. Oficio N° DE-086-22. Óp.. cit.

salario, sin perjuicio de otras sanciones previstas en el régimen disciplinario aplicable al funcionario".

Capítulo XI Derecho de indemnización

En el *Capítulo XI Derecho de indemnización* se modifican:

- Reparación del daño -artículo 81-

El artículo 81 regula la reparación del daño al titular que sufra daños y perjuicios por violación de su derecho a la protección de datos personales. El inciso 2 desarrolla que el ejercicio de las acciones judiciales prescribe en tres años a partir de la existencia del daño. Previamente, este plazo era de un año.

Disposiciones de transitorias:

Se modificó la redacción del Transitorio II, lo cual resultó en el desplazamiento de su anterior texto, al Transitorio III. Su contenido se refiere a que *"la PRODHAB continuará desarrollando sus funciones hasta que estas puedan ser asumidas de forma coordinada por la Agencia de Protección de Datos Personales creada en esta Ley, una vez que al menos su dirección haya sido designada y cuente con capacidad operativa para funcionar, lo que determinará la dirección mediante resolución que deberá ser publicada en el Diario La Gaceta y comunicada al público en general. Dicha transición deberá completarse en un periodo máximo de un año a partir de la entrada en vigor de esta Ley. Todos los procedimientos administrativos que estuvieran en trámite ante PRODHAB serán trasladados a la Agencia de Protección de Datos Personales a partir de que esta entre en funcionamiento, y serán continuados en el estado que estuvieren y hasta su efectiva finalización"*.

V. Consideraciones:

Como se evidenció a lo largo del repaso de los artículos del texto sustitutivo, esta norma es fundamental para la regulación del derecho de protección de datos de las personas en Costa Rica, que garantiza congruencia con los estándares internacionales que rigen la materia. Es claro que de forma efectiva amplía la esfera de protección de las personas, sus derechos e intereses, respecto del manejo de sus datos, especialmente en una sociedad cada vez más digitalizada y automatizada. Además, contrapuesto a esto, se encuentran una amplia gama de obligaciones de los responsables y encargados, que facilitan dicha protección.

En ese sentido, la norma es acorde con los principios y parámetros contenidos en el Reglamento General de Protección de Datos Personales de la Unión Europea[94] y los Estándares de Protección de Datos Personales de la Red Iberoamericana de

[94] 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.

Protección de Datos Personales[95]. Inclusive, en algunas instancias, sus disposiciones son claras adaptaciones de estos instrumentos.

Sobre todo, se considera compatible en aspectos, tales como:

- Definiciones. Al respecto, llama la atención la clasificación de las categorías de datos personales.
  - Principios relativos al tratamiento.
  - Derechos de los titulares de forma general, pero específicamente los derechos ARCO y de portabilidad.
  - Los mecanismos para garantizar la seguridad de los datos.
  - La regulación aplicable a los responsables y encargados del tratamiento.

En consideración con las reformas planteadas, es conveniente impulsar la reorientación de la asignación de recursos humanos, financieros, tecnológicos y otros, para una adecuada gestión, no solo de la Agencia de Protección de Datos, sino de los datos objeto de tratamiento en la Administración Pública.

Asimismo, son imprescindibles las opiniones y valoraciones de los diferentes sectores, de manera que estos puedan brindar sus perspectivas y recomendaciones; que, a su vez, sean analizadas por el órgano legislativo competente para así lograr el objetivo que se desea alcanzar con la presente iniciativa.

VI. Aspectos de técnica legislativa:

Redacción del proyecto de ley

La redacción de la propuesta de ley debe guardar un estilo sumamente parco, desprovisto de palabras innecesarias, donde se establezca una absoluta precisión y la mayor claridad posible. El texto legal debe tener carácter rigurosamente preceptivo; deben omitirse disposiciones que sólo constituyen motivación del texto, enuncian intenciones o son simples recomendaciones.[96] De allí, que el presente texto es acorde con una adecuada técnica legislativa, que cumple con todos los criterios anteriormente mencionados.

Su redacción presenta coherencia y uniformidad a la interpretación que se haga de él. Incluso, se evidencia claridad en cada disposición, que permite una idónea comprensión de los alcances de lo que se pretende regular.
Estructura de la ley

---

[95] Estándares de Protección de Datos Personales para los Estados Iberoamericanos, del 20 de junio de 2017. Los cuales pueden ser consultado en la siguiente dirección web: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
[96] Pérez Bourbon, Héctor. Manual de Técnica Legislativa. - 1a ed. - Buenos Aires: Konrad Adenauer Stiftung, 2007, pág. 102.

Es oportuno considerar los siguientes aspectos sobre la estructura de la ley:

- El objeto de la estructura es hacer fácilmente accesible el conocimiento del contenido de la ley y de las normas en ella contenidas.[97]
  - La redacción, tiende a asegurar que el texto de la ley será interpretado del mismo modo por todos aquéllos que deban utilizarlo.
  - La dinámica legislativa asegura la correcta inserción en el orden jurídico de las normas contenidas en la ley.[98]
- La lógica de los sistemas normativos, procuran evitar las lagunas, contradicciones y redundancias en el orden jurídico.[99]

La finalidad de las reglas sobre estructura consiste en facilitar el acceso del conocimiento del objeto y del alcance de la ley y de las normas en ella contenidas.[100]

El cuerpo del texto sustitutivo del presente proyecto de ley está compuesto por 83 artículos y seis disposiciones transitorias. El cual se encuentra estructurado de la siguiente forma:

---

[97] *"Una buena estructura permite construir un índice de la ley, mediante el cual el usuario, sea profesional o no, puede encontrar rápidamente la norma o el grupo de normas que necesita."* Ibid, pág. 34.

[98] *"La sanción de una nueva ley implicará, necesariamente, una adecuación en el orden jurídico vigente a ese momento: deberán modificarse o derogarse otras normas.*
Un correcto manejo de las reglas referidas a la dinámica legislativa permite una mayor certeza en cuanto a cuáles son las normas que mantienen su vigencia y cuáles las que la han perdido." Ibid, pág. 34.

[99] *"Estos cuatro pilares de la técnica legislativa (estructura, redacción, dinámica y lógica), no obstante, si bien pueden analizarse y estudiarse por separado, confluyen todos ellos al momento de tener que redactar un texto normativo.*
Ello hace que no sea sencillo, en algunos casos, encontrar la ubicación correcta de las reglas que se plantean. En efecto, podrá apreciarse que algunas de ellas vinculadas, por ejemplo, a redacción, tienen decisiva influencia en la estructura o en la dinámica.
Por tal motivo, se ha tratado de señalar, en cada caso, qué otras reglas deben consultarse."
(Estas aclaraciones han sido extraídas, de modo prácticamente textual, de Reglas Prácticas de Técnica Legislativa, de Héctor Pérez Bourbon y otros, pp. 21 y 22.) Ibid, págs. 34 y 35.

[100] *"5. Como consecuencia de lo anterior, las reglas sobre estructura que se indican en este Manual deben ser dejadas a un lado si su cumplimiento conspira contra la clara inteligencia del contenido de la ley.*
6. Al desarrollar la estructura de la ley, debe tenerse muy presente quién será su principal usuario. Si bien todas las leyes deben ser claras en su comprensión, debe ponerse especial cuidado en ello cuando están dirigidas al público en general. En tales casos puede ser necesario que deban reiterarse normas contenidas en otras leyes u otros textos normativos, aun a riesgo de caer en redundancias, pero facilitando el acceso del lego a la totalidad de la normativa sobre la materia en cuestión (ver reglas 207 y 208).
7. En las leyes cuyos principales usuarios serán los profesionales o especialistas, del derecho o de otras disciplinas, esas reiteraciones deben evitarse; asimismo, en estos casos es admisible un cierto grado de dificultad en su comprensión, proveniente de la utilización de términos técnicos (ver reglas 207 y 208).
Un requisito ineludible para lograr el cumplimiento de las leyes es que sean comprendidas por la población. En este aspecto, una buena estructura facilita enormemente la comprensión de la ley.
Sin embargo, las reglas a aplicar en este tema deben ser preponderantemente prácticas y dirigidas al objetivo principal: la fácil accesibilidad al contenido y a la comprensión de la ley. Por ese motivo se han dejado a un lado conceptos que, aunque teóricamente puedan considerarse mejores desde el punto de vista técnico, irían en contra de ese objetivo.
Un ejemplo es el del ámbito temporal de aplicación de la ley. Desde una perspectiva teórica, lo razonable sería que se colocara junto con el ámbito material, el personal y el territorial; no obstante, en prácticamente toda la legislación argentina, el artículo sobre entrada en vigor de la ley se coloca al final. Vano sería entonces pretender una ubicación teóricamente más razonable de dicho artículo si por esa causa quedara ubicado donde nadie lo encontrara sino después de una búsqueda exhaustiva.
Por ello también es que se señala la necesidad de tener presente, en todo momento, quién será el principal usuario. Una ley que regule, por ejemplo, el instituto de Iniciativa Popular, que será utilizada por el común de la ciudadanía, debe ser más fácil de comprender que un código procesal cuyo usuario principal será, seguramente, un profesional del derecho." Ibid, págs. 35 y 36.

Capítulo I Disposiciones generales
- *Artículos 1 a 12*

Capítulo II Principios de protección de datos personales
- *Artículos 13 a 26*

Capítulo III Derechos del titular
- *Artículos 27 a 36*

Capítulo IV Responsable y Encargado del tratamiento
- *Artículos 37 a 44*

Capítulo V Transferencias internacionales de datos personales
- *Artículo 45*

Capítulo VI Medidas proactivas en el tratamiento de datos personales
- *Artículos 46 a 51*

Capítulo VII Disposiciones aplicables a tratamientos concretos
- *Artículos 52 a 60*

Capítulo VIII Agencia de Protección de Datos
- *Artículos 61 a 65*

Capítulo IX Procedimiento en caso de posible vulneración a la normativa de protección de datos
- *Artículos 66 a 71*

Capítulo X Régimen sancionador
- *Artículos 72 a 80*

Capítulo XI Derecho de indemnización
- *Artículos 81 a 83*

Transitorios (I, II, III, IV, V y VI)

Como puede observarse, la estructura de la ley se desarrolla en once capítulos, los cuales están numerados de forma adecuada y con denominaciones que son atinentes al contenido desarrollado por cada uno. Dicho de otro modo, hay congruencia entre el fondo de cada artículo y el tema objeto de los capítulos.

Por otra parte, la ausencia de secciones da mayor claridad de lo que se pretende regular en cada capítulo, al igual que un acceso a la información simplificado.

Título del proyecto de ley

El título de una ley tiene las siguientes características:

> *"El texto debe ser introducido por un título general que precise el objeto de la ley.*
>
> *El título debe ser breve, concreto y reflejar objetivamente el contenido de la ley.*
>
> *Debe evitarse dar a una ley un título ya asignado a otra ley anterior que continúa en vigor.*

El título de la ley es el que el cuerpo legislativo aprueba al momento de su sanción; los títulos puestos por publicaciones, oficiales o no, no reemplazan el título oficial de la ley.

El primer acercamiento que tiene el lector al texto de la ley es, precisamente, el título de la ley. Por ese motivo es importante que la ley tenga un título que le dé suficiente información acerca de qué trata.

Por otra parte, es necesario señalar que muchas veces al publicarse el texto legal se le adiciona un título o nombre; ese nombre o título sólo será el nombre o título de la ley si fue así aprobado por el cuerpo legislativo."[101]

El título en toda ley o proyecto de ley cumple la función de definir o especificar el contenido o finalidad de ésta. Resulta claro que el título del presente proyecto ilustra de forma concreta su contenido, de acuerdo con una correcta técnica legislativa, evitando excederse en palabras innecesarias.

VI. Aspectos de procedimiento:

Votación

De conformidad con lo establecido en el artículo 24 de la Constitución Política, la presente iniciativa de ley requiere para su aprobación de dos terceras partes del total de los miembros de la Asamblea Legislativa.

Asimismo, teniendo presente la opinión emitida por la Corte Suprema de Justicia, donde señaló que la norma se refiere a la organización o funcionamiento del Poder Judicial[102], conforme el artículo 167, de la Constitución Política, se requerirá para apartarse del criterio de la Corte Suprema de Justicia el voto de las dos terceras partes del total de los miembros de la Asamblea.

Delegación

La presente iniciativa no es delegable a una Comisión con Potestad Legislativa Plena, puesto que la propuesta requiere para su aprobación de dos terceras partes del total de los miembros de la Asamblea.

Consultas

---

[101] Ibid, pág. 36.

[102] *"De esta manera, para los efectos de lo establecido en los numerales 167 de la Constitución Política y 59 inciso 1) de la Ley Orgánica del Poder Judicial, debo indicar que el proyecto de ley denominado: Ley de Protección de Datos Personales,* ***sí incide directamente en el funcionamiento y organización del Poder Judicial."*** **Corte Suprema de Justicia.** Oficio N° SP-155-2022 op. cit.

- Obligatorias:

  - Corte Suprema de Justicia.

- Facultativas:

  - Agencia Protección de datos de los Habitantes.
  - Asociación Latinoamericana de internet.
  - Caja Costarricense de Seguro Social.
  - Cámara de Industrias de Costa Rica.
  - Cámara de Tecnologías de Información y Comunicación.
  - Colegio de Ingenieros Químicos de Costa Rica.
  - Colegio de Profesionales en Informática y Computación.
  - Colegio de Profesionales en Sociología de Costa Rica.
  - Colegio de Terapeutas.
  - Comisión Nacional del Consumidor.
  - Contraloría General de la República.
  - Defensoría de los Habitantes.
  - Fundación Privacidad y Datos PRIDAT.
  - Ministerio de Ciencia y Tecnología.
  - Ministerio de Economía, Industria y Comercio.
  - Ministerio de Justicia.
  - Procuraduría General de la República.
  - Sala Tercera de la Corte Suprema de Justicia.
  - Superintendencia de Telecomunicaciones.
  - Tribunal Supremo de Elecciones.
  - UCCAEP.

No se omite manifestar que en la sesión ordinaria N°16 de 10 de noviembre de 2022, de la Comisión Permanente Especial de Ciencia, Tecnología y Educación, se aprobó moción de consulta al texto sustitutivo.

VII. Fuentes:

Constitucionales

- Constitución Política de la República de Costa Rica, del 19 de noviembre de 1949.

- Acuerdo N°399 de 29 de noviembre de 1961. Reglamento de la Asamblea Legislativa.

Leyes y Reglamentos

- Ley N°6227. Ley General de la Administración Pública, de 2 mayo de 1978.

- Ley N°8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales del 5 de setiembre de 2011.

Pronunciamientos administrativos

Otras

- Reglamento General de Protección de Datos (UE) número 2016/679, del 27 de abril de 2016.
- Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de España, número 3/2018, del 5 de diciembre de 2018.

- Estándares de Protección de Datos Personales para los Estados Iberoamericanos, del 20 de junio de 2017.

4. Conclusiones:

Para iniciar estas conclusiones quisiéramos hacer alusión en primera instancia, a los datos personales y las brechas de seguridad.

"Debido a la importancia de los datos y a los beneficios que pueden generarle a los cibercriminales que buscan adueñarse de ellos, continuamente observamos brechas de seguridad relacionadas con la fuga de información, en los cuales se utilizan distintos vectores de ataque para lograr los fines maliciosos.

Por ejemplo, en 2014 se conocieron casos de fuga de información relacionados con malware Point of Sale*, en compañías como* Target*,* Home Depot *o* UPS*, donde los atacantes lograron obtener más de 40 millones de números de tarjetas de crédito y débito de usuarios. Empresas como* eBay *o* Yahoo!*también se vieron en la necesidad de notificar a miles de usuarios que sus cuentas y contraseñas habían sido filtradas a través de un ataque.*

En 2015 otras industrias también se han visto afectadas, tal es el caso de Comunity Health System*(CHS) en los Estados Unidos, que fue víctima de la fuga de 4.5 millones de registros médicos. De acuerdo con el comunicado de la entidad, sus sistemas fueron víctimas de una APT. Otro de los casos más conocidos este año, fue el robo de datos confidenciales a Ashley Madison, sitio de citas*online *especializado en relaciones extramaritales, que puso en potencial peligro a sus 37 millones de usuarios. Sin importar las actividades de las empresas, la industria a la que pertenezcan, su tamaño o ubicación geográfica, e independientemente del ataque utilizado para afectarlas,* ***la consecuencia más común suele ser la fuga de información****, con los conocidos daños a la imagen de las organizaciones. En esta lista se cuentan empresas, gobiernos y otras entidades, impactado de manera negativa a sus miles, e incluso millones de usuarios.*

Por estas razones, en distintos países se han emitido leyes orientadas a la protección de los datos personales, que deben cumplir entidades del sector público o privado que traten información de carácter personal. La protección de los datos es un derecho ciudadano, que brinda la facultad para controlar a voluntad la información personal de cada individuo, que es almacenada, procesada o transmitida por terceros" (https://www.uv.mx/infosegura/general/conocimientos_datospersonales/)

Es casualmente tal y como lo indicaban las líneas anteriores, que hoy la protección de los datos debe resguardase a toda costa, y de ahí la importancia que reviste este proyecto de ley. en ningún momento de la historia del ser humano, lo concerniente a los datos personales y su protección han tenido mayor importancia que en la actualidad. En la era digital en la cual nos encontramos inmersos, la obtención, así como el almacenamiento de información personal son aspectos esenciales.

Esta iniciativa de ley es una importante y necesaria reforma, que lleva estrecha coincidencia con la reforma constitucional, que se le pretende hacer al artículo 24 de nuestra Constitución Política que también en este mismo momento, está siendo discutida y forma parte importante del orden del día del Plenario Legislativo, al incluir el derecho fundamental a la protección de datos personales y reemplazar el concepto de intimidad por el de vida privada.

Esta normativa la requiere nuestra sociedad, ya que cada vez, para el ciudadano, sus datos privados pueden verse vulnerados por un sinfín de razones, lo que pone en peligro sus bienes materiales y, en otros casos, su dignidad humana o su prestigio profesional y laboral, incluso su identidad personal.

En este orden de ideas, es importante establecer a qué riesgos nos referimos cuando hablamos de protección de datos personales o más bien sería a la vulneración de nuestros datos personales; es por ello que traemos un concepto de riesgos aplicada a esta materia, de Juan Francisco Rodríguez Ayuso, en su libro *Figuras y responsabilidades en el tratamiento de datos personales*," En materia de protección de datos, el riesgo consistiría en la probabilidad de que suceda un daño para el interesado como resultado de la realización de operaciones de tratamiento sobre sus datos personales." (Rodríguez,2019, 171).

De la definición anterior, se puede entrever que la importancia de la protección de datos personales radica en la vulneración y en la violación de nuestros derechos y libertades fundamentales, es decir, produciéndonos un daño por no existir un adecuado tratamiento en el manejo de nuestros datos, así como a quiénes les entregamos nuestra información personal. Es por ello, como lo destaca Juan Francisco Rodríguez Ayuso, *"que es fundamental tener en cuenta el riesgo que implica cualquier tratamiento de datos personales, así como cualquier otro riesgo que pueda derivarse de situaciones tales como violaciones de seguridad, que pueden acarrear daños y perjuicios físicos, materiales o inmateriales para las personas físicas, tales como pérdida de control sobre sus datos personales o limitaciones de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización (de acuerdo con el*

Reglamento (UE) 2016/679 en su artículo 4.5 establece: 'la seudonimización es 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'), daños para la reputación, pérdida de confidencialidad de datos personales, sometidos al secreto profesional o cualquier otro perjuicio económico o social relevante para nosotros.*" (Rodríguez,* Op. Cit.*, 172).*

Aprobar esta iniciativa le posibilitaría a Costa Rica, subir la protección de datos al más alto estándar internacional en la materia y remozar completamente el marco normativo para devolverle a las personas el control sobre su información personal y evitar que el ciudadano pueda sufrir *daños y perjuicios físicos, materiales o inmateriales.*

En el capítulo II de este proyecto de ley, quedan regulados entre otras muchas cosas, los principios de protección de datos personales y se recoge 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. Refuerza, por tanto, los derechos fundamentales de la "Vida Privada", la "Protección de los Datos Personales", la "Libertad" y el "Secreto de las Comunicaciones".

Para la elaboración del mismo se hizo una revisión exhaustiva de las múltiples consultas que se recibieron, luego de presentado el texto sustitutivo, por ello es menester indicar que muchas de ellas, y sobre todo las más relevantes en materia de fondo serán presentadas vía moción de fondo para mejorar el texto sustitutivo presentado en el mes de noviembre del año pasado. Se ha hecho un trabajo conjunto con expertos en el tema, para valorar certeramente lo que reviste de la mayor relevancia en este tópico y también lo que es propicio incluir.

Es menester indicar que al final del proceso de análisis de este expediente se hicieron una serie de mociones de fondo para mejorar aún más el texto sustitutivo presentado, acogiendo éstas las recomendaciones que hicieron las entidades directa e indirectamente involucradas, en especial MIDEPLAN y la Contraloría de la República, luego de que se volviera a consultar el texto sustitutivo. Esto permite que el texto este afinado y con inclusiones muy valiosas a lo largo del mismo, tocando estas modificaciones partes esenciales en el manejo de la protección de los datos para el país.

También es valioso rescatar, que, para llegar a este texto final, se tuvo la participación de personas de peso en el tema en el país, con la finalidad de que el documento estuviera a la altura de la legislación a nivel internacional.

Finalmente, esta iniciativa de ley constituye un sello de seguridad para los ciudadanos costarricenses en cada una de sus actividades personales, tales como:

la confidencialidad o inviolabilidad del hogar, el lugar donde se ejerce la ocupación habitual, la correspondencia, las comunicaciones, las relaciones familiares, la sexualidad y su intimidad, lo cual es parte esencial del ser humano.

VIII. Recomendaciones:

Con base en las consideraciones anteriores, las suscritas diputaciones, miembros de la Comisión Permanente Especial de Ciencia, Tecnología y Educación, rendimos el presente Dictamen Afirmativo de Mayoría y recomendamos respetuosamente al Plenario la aprobación del expediente en discusión.

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, independientemente de su nacionalidad.

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 del país.

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 o plazos desproporcionados, teniendo en cuenta factores como los costos y el tiempo

necesario para la identificación o reidentificación de la persona a la luz de la tecnología disponible en el momento del tratamiento.

b. Base de datos: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado, independientemente de que los datos se encuentren respaldados en soportes físicos o electrónicos.

c. Cesión de datos: toda revelación de datos realizada a una persona, entidad u organización distinta del Titular.

d. Consentimiento: manifestación de la voluntad, libre, específica, inequívoca e informada del Titular de los datos personales o su representante, a través de la cual acepta, mediante una 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 de una persona física que permitan o confirmen su identificación única, tales como imágenes faciales o datos dactiloscópicos, entre otros.

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. Se consideran sensibles los datos personales que revelen el origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; condición socioeconómica, 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 en el ámbito público o privado, 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 que pueden ser accedidas por cualquier persona. Se entienden como fuentes de acceso público, las siguientes: 1) bases de datos de personas jurídicas, bienes inmuebles, bienes muebles, catastro y propiedad industrial del Registro Nacional, 2) los registros de nacimientos, matrimonios y defunciones del Registro Civil, 3) las bases de datos que acrediten la condición de colegiado a un colegio profesional o la habilitación o des habilitación de personas físicas para el ejercicio de determinados oficios, como el notariado, la condición de perito, curador o similares, 4) el diario oficial La Gaceta y el Boletín Judicial, independientemente del soporte físico o digital en el que se publiquen, 5) Las publicaciones realizadas en medios masivos de comunicación, entendiendo por tales los provenientes de la prensa, cualquiera sea el soporte en el que figuren o el canal a través del cual se practique la comunicación, 6) Las guías, publicaciones, anuarios, directorios y similares que tengan la finalidad comunicar públicamente la pertenencia de determinadas personas a organizaciones gremiales, asociaciones, colegios profesionales u otras organizaciones de la sociedad civil, en el tanto cuenten con el consentimiento del Titular y se cumpla la finalidad para la que dicho consentimiento fue otorgado por el Titular. El funcionamiento de las bases de datos de acceso público respetará los términos de la presente Ley, en especial en cuanto a los principios de legitimación y minimización.

m. Grupo económico: agrupación de sociedades o empresas, de hecho o de derecho, que se manifiesta mediante una unidad de decisión, es decir, la reunión de todos o una parte sustancial de los elementos de mando o dirección empresarial por medio de un centro de operaciones, y que se exterioriza mediante dos movimientos básicos: el criterio de unidad de dirección, ya sea por subordinación o por colaboración entre sus miembros, o el criterio de dependencia económica de sus miembros, sin importar que su personalidad jurídica se vea afectada, o que su patrimonio sea objeto de transferencia.

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 económico 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. Seudonimización: 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 Titular del dato, del Responsable del tratamiento, del 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 o interesado: persona física a quien le conciernen los datos personales.

u. 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, cesión, transferencia, difusión, posesión, aprovechamiento, cotejo, interconexión, limitación, supresión, destrucción, y; en general, cualquier uso o disposición de datos personales.

v. Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos 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 en sentido amplio, 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. También se aplicará al tratamiento de datos personales, incluso cuando los datos personales no formen parte o no estén almacenados en una base de datos.

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.

ARTÍCULO 5.- Datos de personas fallecidas

1. En caso de fallecimiento del Titular de los datos, los derechos que reconoce la presente Ley pueden ser ejercidos por sus herederos, que, previa acreditación de su condición, 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, los herederos 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.

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 económico, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo económico, 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. No se podrá limitar el derecho a la protección de datos personales mediante ley, salvo de manera excepcional, cuando existan razones que justifiquen su necesidad, sean adecuadas y proporcionales en una sociedad democrática, y respeten los derechos y las libertades fundamentales de los Titulares.

2. 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.

3. 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, cesiones 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.

ARTÍCULO 8.- Tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y cesiones interinstitucionales de datos en el sector público

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, que no deberán ser menores a las garantías y derechos establecidos en esta Ley.

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 cesión solo se llevará a cabo previa autorización de la Agencia de Protección de Datos, quien deberá verificar, en un plazo no mayor a 10 días hábiles, el cumplimiento de las siguientes condiciones acumulativas:

i) la cesión 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 cede los datos los haya obtenido con fundamento en una de las bases legales previstas en el artículo 15 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 cesión sean únicamente los adecuados y estrictamente necesarios para acometer la finalidad pública, de conformidad con el principio de minimización de datos. Se prohíbe la cesión o transferencia masiva e indiscriminada de bases de datos.

4. En cualquiera de los anteriores supuestos, las cesiones 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 cesión. Además, la cesión debe documentarse en un convenio interinstitucional que deberá ser comunicado a la Agencia de Protección de Datos Personales, publicado y puesto a disposición de la ciudadanía para su escrutinio,

mediante los medios que se disponga vía Reglamento, resguardando la confidencialidad de los datos personales involucrados en la cesión

5. Las transferencias o cesiones 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, el ejercicio del poder público y potestades de fiscalización de la función pública, ni en aquellos casos donde la revelación de la transferencia o cesión a los Titulares pueda comprometer seriamente el objetivo de interés público perseguido con la transferencia o cesión. No obstante, lo anterior, el Titular tendrá derecho a conocer si sus datos fueron objeto de transferencia o cesión cuando cese el riesgo de que dicha revelación comprometa el interés público antes indicado.
6. No se considerará cesión ni transferencia de datos la remisión de datos personales realizada por un Responsable o Encargado del sector público ante una orden de una autoridad judicial competente en el marco de sus facultades legales, siempre que dicha orden se realice dentro de una investigación o procedimiento específico.

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, condición socioeconómica, 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 razonablemente necesarios para el ejercicio y cumplimiento de atribuciones y obligaciones previstas en una norma legal o en un contrato libremente consentido por el Titular de los datos.

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 para uno o más fines especificados, consentimiento que podrá derivar de un contrato donde el tratamiento de tales datos sensibles resulta indispensable, siempre que así conste que se haya informado al Titular.

e. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros, fundadas 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, investigación en salud, 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, como pandemias debidamente declaradas por las autoridades de salud competentes, 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.

i. El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable o del Titular en el ámbito del derecho laboral, de la seguridad social o ayudas sociales, en la medida en que así lo autorice el marco normativo y establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del Titular.

j. El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los Titulares;

k. El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

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 y/o el Ministerio de Justicia.

2. Además de los funcionarios judiciales involucrados, los abogados en ejercicio podrán realizar tratamiento de datos personales referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas cuando tengan por objeto tratar la información tratada por sus clientes para el ejercicio de sus funciones, bajo la obligación de secreto profesional.

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 fines lícitos, y de conformidad con los principios de finalidad y minimización previstos en esta Ley, 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.

CAPÍTULO II

PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 13.- Principios aplicables al tratamiento de datos personales

El tratamiento de datos personales deberá realizarse conforme a los principios de exactitud, legitimación, lealtad, transparencia, limitación de la finalidad, minimización, responsabilidad proactiva, seguridad y confidencialidad.

ARTÍCULO 14.- Principio de exactitud

1. Los datos serán exactos, y si fuere necesario, actualizados. No será imputable al Responsable, 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 recolectó 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.

2. En todos los casos anteriores el Titular tendrá derecho de solicitar rectificación de sus datos personales.

ARTÍCULO 15.- Principio de legitimación

1. El tratamiento de los datos personales será legítimo solo cuando se realice con fundamento en alguna de las siguientes bases de legitimación:

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 y 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 una 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. Los supuestos establecidos en los incisos b, c, f y h estarán sujetos al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad.

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 participación 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 o excedan las expectativas razonables del Titular respecto a sus finalidades.

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. La existencia de cesiones y/o transferencias internacionales de datos personales, los destinatarios, las categorías de datos y 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 de tratamiento de datos personales que recojan los principios y disposiciones establecidas en esta Ley.

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, análogas o compatibles 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 y adoptará todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos.

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, el Responsable podrá conservar los datos más allá del plazo de conservación en cumplimiento de un interés legítimo, para el cumplimiento de la finalidad inicial de su tratamiento y con pleno respeto a los derechos y garantías del Titular. Asimismo, la ley podrá establecer excepciones respecto al plazo de conservación de los datos personales. De igual forma, se entenderán válidas las excepciones contenidas en leyes especiales en materia de archivo, investigación o estadística.

ARTÍCULO 23.- Principio de responsabilidad proactiva

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 cesiones o transferencias de datos personales.

3. Entre los mecanismos que el Responsable podrá adoptar para cumplir con el principio de responsabilidad proactiva 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 medidas para el análisis de los riesgos asociados al tratamiento de datos personales, y en caso de que corresponda, evaluaciones de impacto 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 en los plazos establecidos en esta Ley.

h. Llevar el registro de tratamiento de datos personales, cuando corresponda conforme lo establecido en esta Ley.

i. Designar un oficial de protección de datos personales.

4. El Responsable revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad proactiva, 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 y el Encargado establecerán y mantendrán, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y

técnico suficientes para mantener 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.

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 violación de la seguridad de los datos personales para los Titulares.

i. La violación de la seguridad de los datos personales 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.

ARTÍCULO 25.- Notificación de violación a la seguridad de los datos personales

1. Cuando el Responsable tenga conocimiento de una violación 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, aun cuando ocurra de manera accidental, notificará a la Agencia de Protección de Datos Personales y a los Titulares afectados en un plazo de 72 horas, desde que se tuviera conocimiento efectivo, sin dilación alguna.

2. La notificación a los Titulares no resultará aplicable cuando el Responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la violación de seguridad ocurrida, o bien, que se cumple alguna de las siguientes condiciones:

a. Cuando el Responsable ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b. Cuando el Responsable ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del Titulares involucrados;
c. Cuando suponga un esfuerzo desproporcionado para el Responsable. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los Titulares.

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, tanto a la Agencia de Protección de Datos como a los Titulares afectados, contendrá, al menos, la siguiente información:

a. La naturaleza del incidente.

b. Los datos personales que pueden considerarse 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 a disposición del 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 presentar actualizaciones periódicas a la Agencia de Protección de Datos Personales sobre el informe inicial, cada vez que se disponga de información nueva o diferente sobre el incidente, hasta la fecha en que la investigación del incidente haya concluido y que el incidente asociado se haya mitigado y resuelto por completo.

5. El Responsable documentará toda violación 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 violación; 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 violaciones 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.

3. Los derechos del Titular son irrenunciables. Será nula de pleno derecho toda estipulación en contrario.

ARTÍCULO 28.- Disposiciones generales sobre ejercicio de los derechos

1. Los derechos reconocidos en este Capítulo se ejercerán por medio escrito, y serán comunicados al Responsable en los medios que hubiese puesto a disposición del Titular, por medio del oficial de protección de datos (de haberlo), o, en su defecto, en su domicilio social o establecimiento comercial abierto al público. 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. Salvo que otro plazo se estableciera en esta Ley, la respuesta a una solicitud de ejercicio de derechos por parte de un afectado deberá comunicarse en un plazo de cinco días hábiles posteriores a su recepción, al medio señalado por el afectado.

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, previa acreditación de su identidad, tendrá derecho de obtener del Responsable del tratamiento en el plazo de cinco días hábiles, confirmación de si se están tratando o no sus datos personales, y en tal caso, derecho de acceso en el mismo plazo indicado a los datos personales y a la siguiente información:

a. Las finalidades del tratamiento y las bases legales que las legitiman.

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

c. Los destinatarios o las categorías de destinatarios a los que se cedieron o se prevean ceder los datos personales.

d. Información sobre las transferencias internacionales de datos que se hayan efectuado o se prevean efectuar, incluyendo los países de destino.

e. El plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.

f. 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 o a presentar una reclamación ante la Agencia de Protección de Datos Personales.

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

h. La existencia o no de decisiones automatizadas respecto del tratamiento de sus datos personales, incluida la elaboración de perfiles.

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 facilitará una copia de los datos personales objeto de tratamiento. El Responsable podrá cobrar un canon razonable basado en los costos administrativos, por cualquier otra copia solicitada por el Titular. 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 o supresión

1. El Titular tendrá derecho a obtener del Responsable del tratamiento y en el plazo de cinco días hábiles, la cancelación de sus datos personales, 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 recolectados.

b. El Titular revoque el consentimiento en que se basa el tratamiento, y este no se ampare en otra base legal.

c. El Titular haya ejercido su derecho de oposición con arreglo al artículo 32, y no prevalezcan otros motivos legítimos para el tratamiento.

d. Los datos personales hayan sido tratados ilícitamente.

e. Los datos personales deban suprimirse para el cumplimiento de una obligación legal o por orden de una autoridad competente.

2. El apartado 1 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.

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.

f. Cuando los datos personales deban ser conservados durante los plazos previstos en disposiciones legales o contractuales, entre el Responsable o Encargado del tratamiento y el Titular de los datos.

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 publicidad, la prospección comercial o la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.

2. El Responsable del tratamiento deberá responder la solicitud en el plazo máximo de cinco días hábiles, y 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 una decisión basada en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos o afecten sus intereses de manera significativa, destinadas a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o

predecir, en particular, su rendimiento profesional, situación económica o crediticia, 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, siempre que no se revelen con dicha explicación secretos comerciales; así como 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, particularmente cuando se basen en datos sensibles, según son definidos en esta Ley.

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 al Responsable 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. Será improcedente el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad en los siguientes casos:

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 expresamente establecidas en la ley.

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 cargo 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 del Responsable del tratamiento

1. Los Responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley, sus normas reglamentarias y otras que rijan su actividad:

a. Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y sus normas reglamentarias, especialmente los derechos de los Titulares y la materialización de los principios del tratamiento de datos personales;

b. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de protección de datos, especialmente conocer, actualizar, rectificar, suprimir sus datos personales u oponerse al tratamiento de los mismos;

c. Cumplir debidamente con el deber de informar al Titular sobre la finalidad de la recolección y sus derechos;

d. Tratar los datos personales bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e. Implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos, exactos y comprobables;

f. Actualizar los datos personales, rectificar la información cuando sea incorrecta y adoptar medidas necesarias para que la misma se mantenga actualizada;

g. Tramitar debidamente las solicitudes presentadas por el Titular, respondiéndolas de manera completa y oportunamente;

h. Realizar la notificación de violaciones de seguridad en los términos y plazos previstos en esta Ley.

i. Cumplir las instrucciones, órdenes o requerimientos que imparta la Agencia de Protección de Datos Personales.

j. Formalizar mediante la suscripción de un acuerdo, contrato o cualquier otro instrumento jurídico la prestación de servicios entre el Responsable y el Encargado, en entre corresponsables.

k. Verificar que los Encargados, o quienes éstos subcontraten, ofrecen garantías suficientes para realizar el tratamiento de datos personales conforme con los requisitos de la presente Ley y garantice la protección de los derechos del Titular. Dicha verificación debe realizarse con anterioridad a la contratación u realización de otro acto jurídico que lo vincule con el Encargado;

l. Exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y debido tratamiento de la información del Titular;

2. Para la adopción de las medidas a que se refiere el apartado anterior los Responsables 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.- Cesión de datos

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, en alguno de los supuestos previstos en el artículo 15.1 de esta Ley, y siempre que dicha cesión sea informada al Titular.

2. Aquel a quien se cedan los datos personales se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley, y a facilitar al Titular de los datos personales cedidos la siguiente información, dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos:

a) la identidad y los datos de contacto del Responsable y, en su caso, de su representante;

b) los datos de contacto del oficial de protección de datos, de haberlo;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del Responsable de transferir datos personales a un destinatario en un tercer país.

3. Las disposiciones del apartado anterior no serán aplicables cuando y en la medida en que:

a) el Titular ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. En tales casos, el Responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del Titular;

c) la obtención o la comunicación esté expresamente establecida en una ley, o;

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional emanada en una norma de carácter legal.

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 cesión ni 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 Titulares 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, siempre que sea mediante la adopción de un acto administrativo 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, cuya formalización será responsabilidad del Responsable.

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 sin dilación alguna al Responsable cuando ocurra una violación de la seguridad de los datos personales que trata por sus instrucciones.

e. Informar sin dilación alguna 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 y garantizar que su personal y cualquier persona autorizada por el Encargado para

tratar datos personales del Responsable cuenten con obligaciones contractuales o derivadas de una obligación legal que les obliguen a respetar la confidencialidad 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 ceder 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, así como facilitar la información necesaria para demostrar el cumplimiento de las obligaciones en el presente artículo, sea en el marco de una auditoría realizada al Responsable, de un procedimiento de fiscalización por una autoridad competente o cuando dicha obligación derive del contrato de encargo.

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 de datos personales 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 cedieron o cederán 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.

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 de datos personales 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. 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.

c. 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 y 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 instituciones 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.

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. Regla general sobre transferencias internacionales de datos: 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 encargad 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. Casos en los que la transferencia internacional de datos es procedente: El Responsable y Encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:

a. Consentimiento del Titular: Cuando el Responsable cuente con el consentimiento informado del Titular de los datos.

b. Transferencia fundamentada en un tratado internacional: Cuando la transferencia sea exigida legalmente o en un tratado internacional del que la República de Costa Rica sea parte.

c. Transferencia fundamentada en una decisión de adecuación: 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, que no podrán ser menores que las reconocidas en la presente Ley.

d. Transferencias fundamentadas en garantías adecuadas del exportador: Cuando el exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y acredite el cumplimiento de condiciones mínimas suficientes, derechos exigibles y el acceso a acciones legales efectivas. Se considerarán como garantías suficientes el cumplimiento de alguna de 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 principios y derechos de los Titulares.

ii) Que el exportador y destinatario adopten un esquema de autorregulación vinculante, normas corporativas vinculantes, código de conducta o un mecanismo de certificación local o internacionalmente reconocidos, siempre y cuando estos sean acordes con las disposiciones previstas en esta Ley.

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 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.
4. Cuando el Titular de forma libre, voluntaria y por su propia iniciativa, transfiera sus datos a un Responsable situado en una jurisdicción diferente a la del Titular.

CAPÍTULO VI

MEDIDAS PROACTIVAS EN EL TRATAMIENTO DE DATOS PERSONALES

ARTÍCULO 46.- Reconocimiento de medidas proactivas

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. Teniendo en cuenta el estado de la técnica, el costo de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entrañe el tratamiento de los datos para los derechos y libertades de los Titulares, 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, en aplicación del principio de responsabilidad proactiva y cuando lo estime conveniente, podrá designar a un oficial de protección de datos personales.

2. Los Responsables que designen un oficial de protección de datos, deberán poner a disposición del Titular sus datos de contacto en cualquier aviso o política de privacidad de la que disponga.

3. 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, y siempre que las otras funciones que desempeñen no den lugar a un conflicto de interés. 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.

4. El Responsable o el Encargado estarán obligados a respaldar al oficial de protección de datos personales, de haberlo, 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.

5. El oficial de protección de datos personales, de haberlo, desempeñará al menos, las siguientes funciones:

a. Informar y asesorar al Responsable o el Encargado 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 y del Encargado el cumplimiento de la legislación aplicable en la materia y de sus políticas.

6. Cuando se trate de una persona física integrada en la organización del Responsable o Encargado del tratamiento, el oficial de protección de datos no deberá 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.

7. 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 o el Encargado la existencia de cualquier deber de confidencialidad o secreto.

8. Cuando el oficial de protección de datos tenga conocimiento de la existencia de una violación de seguridad en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del Responsable o Encargado.

9. El oficial de protección de datos personales estará obligado por el secreto profesional y el deber de confidencialidad en lo que respecta al desempeño de sus funciones establecidas en esta Ley."

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

1. Cuando el Responsable o Encargado 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 cinco días hábiles 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 cinco días hábiles.

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 y el Encargado podrán 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 elaborados por las asociaciones y otras organizaciones, nacionales o internacionales, de alcance general o sectoriales.

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 o relativos a condenas e infracciones penales previstos en esta Ley.

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

4. La Agencia de Protección de Datos deberá 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. 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 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 Agencia de Protección de Datos 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 suspenderle hasta que la Agencia de Protección de Datos 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 el uso de sistemas de identificación biométrica en tiempo real en espacios públicos a través de cámaras o sistemas de video vigilancia que tengan por finalidad la identificación indiscriminada o masiva de las personas.

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 del sector público o privado, 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 del sector público o privado, 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 del sector público o privado, tales como vestuarios, servicios sanitarios, salas de lactancia, 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 del sector público o privado 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 del sector público o privado 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.- Datos relativos al comportamiento crediticio del sector financiero y no financiero

1. Los datos personales relativos al comportamiento crediticio tratados por el Centro de Información Crediticia (CIC) se regirán por las normas dictadas por la Superintendencia General de Entidades Financieras respetando las garantías, principios y derechos concedidos en esta Ley, 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. Esto sin perjuicio del tratamiento que sobre datos crediticios puedan hacer otros Responsables del sector no financiero, en los términos indicados en el presente artículo y respetando el principio de minimización establecido en esta Ley.

2. Queda expresamente autorizado el tratamiento de datos personales relativos al comportamiento crediticio cuando tengan la finalidad de informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos datos relativos al cumplimiento o

incumplimiento de obligaciones de carácter comercial y/o crediticio que permitan evaluar los riesgos de contratación, la conducta comercial y/o la capacidad de pago del Titular. Lo anterior, en los casos en que dichos datos personales sean obtenidos de fuentes de acceso público, y/o procedentes de informaciones facilitadas por el acreedor con base en su interés legítimo prevalente, o en las circunstancias previstas en la presente Ley.

3.Cuando se realice una cesión de datos personales para el fin indicado en el párrafo anterior, el acreedor, en calidad de Responsable de los datos, deberá mantener un registro del Titular de los datos cedidos, que podrá ser requerido por la Agencia de Protección de Datos en el marco de una investigación o procedimiento sancionatorio.

4. Los datos personales relativos al comportamiento crediticio que sean significativos para evaluar la solvencia económica o financiera podrán conservarse durante el plazo que resulte necesario, y como máximo, podrán conservarse hasta por cuatro años, desde el vencimiento del plazo original de la operación de crédito. El plazo se reduce a dos años cuando el deudor cancele o extinga la obligación, plazo a contar a partir de la fecha en que lo hace, debiendo constar esta información en el informe crediticio.

5. Cuando se cancele una obligación incumplida registrada en una base de datos de solvencia, o exista una orden judicial o administrativa que así lo ordene, el acreedor de la obligación deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo a todos los Responsables de bases de datos de solvencia a quienes hubiera informado sobre el incumplimiento de la obligación por parte del deudor. Una vez recibida la comunicación por el Responsable de la base de datos de solvencia, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación en el informe crediticio.

6. Los Responsables de las bases de datos relativos al comportamiento crediticio deberán en todo momento velar por realizar valoraciones objetivas de la información, sin que esta pueda prestarse para ningún tipo de discriminación. Dichas condiciones serán supervisadas por la Agencia de Protección de Datos.

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. 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.

c. 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.

d. 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) Para que responda por el cumplimiento de las obligaciones derivadas de esta Ley, 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.

e. 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 ético de la investigación previsto en la Ley 9234 Ley Reguladora de Investigación Biomédica. 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 10 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 es la autoridad nacional de control encargada de la regulación y protección de los datos personales de los habitantes de la República.

2. Será un órgano desconcentrado del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt). Contará con grado de desconcentración administrativa con idoneidad especial y técnica, dotada de independencia operativa, técnica, administrativa 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 Marco de Empleo Público, No. 10.159.

Su organización se definirá reglamentariamente y ajustará sus actuaciones a las disposiciones contenidas en esta Ley.

3. Podrá celebrar todo tipo de contratos y convenios permitidos por la ley, 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.

4. Sus decisiones darán por agotada la vía administrativa, sin que pudieran impugnarse las resoluciones ante el MICITT ni ser avocadas sus competencias por este.

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. La denominación salario base utilizada en esta Ley debe entenderse como la contenida en el artículo 2 de la Ley No. 7337 de 5 de mayo de 1993.

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, en los términos que establezca el reglamento a esta Ley. No se aceptarán donaciones de empresas que se dediquen a la comercialización de datos personales, sean nacionales o internacionales.

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

d. Los ingresos producto del canon que establece la presente 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 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. Emitir criterio 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. Investigar, resolver y sancionar, de oficio o a ante denuncia, cualquier infracción atribuida a una persona física o jurídica, del sector público o privado, e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.

g. Promover acciones de cooperación y armonización normativa con autoridades de protección de datos personales de otros países y entidades u

organismos internacionales; celebrar convenios de cooperación y contratos con organizaciones públicas o privadas, nacionales o extranjeras, en el ámbito de su competencia, para el cumplimiento de sus funciones; cooperar con autoridades de protección de datos personales de otros países en la sustanciación de procedimientos sancionatorios, en particular, coordinando sus investigaciones o intervenciones o llevando a cabo acciones conjuntas, y proveyendo asistencia para el ejercicio de los derechos establecidos en esta Ley

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.

l. Emitir dictámenes no vinculantes a solicitud de interesados, con el objeto de brindar criterios generales sobre el cumplimiento de las obligaciones y ejercicio de derechos contemplados en esta Ley y los reglamentos que la desarrollen.

m. Gestionar y administrar sus recursos y presupuesto, para lo que podrá aprobar los contratos de obras y servicios, de acuerdo con el ordenamiento jurídico vigente.

n. Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales.

o. Todas aquellas otras que le conceda la presente Ley.

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.

i. Dictar y ejecutar medidas cautelares en sede administrativa para garantizar la protección de los datos personales de los habitantes.

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, salvo en el caso de auditorías preventivas, en cuyo caso podrá actuar sin comprobación previa de indicios.

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 determinadas funciones técnicas sustantivas como administrativas, y que, en ausencia temporal de la Dirección, le sustituirá en todas sus funciones. La Dirección ejercerá sus funciones con plena independencia y objetividad

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.

Tienen impedimento para ser nombrados como Director y/o Adjunto los parientes, hasta tercer grado de consanguinidad o afinidad del presidente de la República, los vicepresidentes, los ministros y viceministros o con vínculo civil por afinidad hasta el mismo grado.

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 por un plazo superior a seis meses.

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, incluso en grado de tentativa.

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 cesión o transferencia internacional comportará 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, en el cuanto su responsabilidad no se derive de instrucciones giradas por el Responsable, o del incumplimiento de este a las disposiciones de esta Ley o su reglamento.

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 cinco y diez salarios base.

b. Para las faltas graves, una multa de diez a cincuenta salarios base.

c. Para las faltas gravísimas, una multa de cincuenta hasta cien salarios base, y, en caso de personas físicas o jurídicas que cometieran la infracción en el ejercicio de una actividad lucrativa, el monto superior entre cien 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.

ARTÍCULO 74.- Infracciones consideradas gravísimas

1. Se consideran gravísimas 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 10 de esta Ley

f. El tratamiento de datos personales relacionados con condenas e infracciones penales fuera de los supuestos permitidos por el artículo 11 de esta Ley."

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

h. 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.

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

j. 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.

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

l. 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 la presente Ley.

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

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

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 cesión 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, cancelación o 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 los datos personales de las que tuviera conocimiento.

l. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos personales 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. 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 cedido o transferido 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 hubiere sido designado.

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 seis 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. Haber designado de manera proactiva a un oficial de protección de datos, en los términos previstos en esta Ley.

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 descentralizada, 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. Los funcionarios públicos que incurran en algunas de las infracciones establecidas en los artículos 74, 75 y 76 y se haya demostrado la culpa o dolo en su accionar u omisión, serán sancionados con la suspensión de su cargo por hasta noventa días, sin goce de salario, sin perjuicio de otras sanciones previstas en el régimen disciplinario aplicable al funcionario. 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 tres años 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, mediante las entidades competentes, en un plazo máximo de doce meses contados a partir de la publicación de esta Ley, deberá concretar el traslado de los recursos, bienes y personal de la PRODHAB a la Agencia de Protección de Datos Personales, e iniciar los procedimientos para el nombramiento de los puestos de dirección de esta, en los términos previstos por esta Ley.

TRANSITORIO II.- La PRODHAB continuará desarrollando sus funciones hasta que estas puedan ser asumidas de forma coordinada por la Agencia de Protección de Datos Personales creada en esta Ley, una vez que al menos su dirección haya sido designada y cuente con capacidad operativa para funcionar, lo que determinará la dirección mediante resolución que deberá ser publicada en el Diario La Gaceta y comunicada al público en general. Dicha transición deberá completarse en un periodo máximo de doce meses a partir de la publicación de esta Ley. Todos los procedimientos administrativos que estuvieran en trámite ante PRODHAB serán trasladados a la Agencia de Protección de Datos Personales a partir de que esta entre en funcionamiento, y serán continuados en el estado que estuvieren y hasta su efectiva finalización.

TRANSITORIO III. El siguiente Presupuesto Ordinario de la República que formule el Poder Ejecutivo después de la publicación de esta Ley, deberá reflejar el traslado de las partidas presupuestarias del programa presupuestario de la PRODHAB hacia

el título presupuestario que se creará, correspondiente a la Agencia de Protección de Datos. La Dirección de la Agencia de Protección de Datos Personales continuará con la misma base salarial que mantiene la Dirección de la PRODHAB, y se tomará como base para el establecimiento de la nuestra estructura de puestos.

TRANSITORIO IV. 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 a partir de la publicación de esta Ley para adecuar su funcionamiento y tratamiento de datos personales a las disposiciones de esta Ley.
TRANSITORIO V. La Agencia de Protección de Datos emitirá la reglamentación requerida de esta Ley en el plazo de doce meses después de su entrada en funcionamiento.

TRANSITORIO VI. La Superintendencia General de Entidades Financieras dictará las regulaciones requeridas de acuerdo al artículo 55 de esta Ley, en el plazo de doce meses a partir de la publicación de esta Ley.

Rige doce meses posteriores a su publicación.

Dado en la Sala Plena II de la Asamblea Legislativa. Área de Comisiones Legislativas V, a los nueve días del mes de febrero del año dos mil veintitrés.

José Joaquín Hernández Rojas

Jorge Antonio Rojas López

Kattia Cambronero Aguiluz

Kattia Rivera Soto

José Pablo Sibaja Jiménez

Rocío Alfaro Molina

Leslye Rubén Bojorges León

DIPUTADAS Y DIPUTADOS

Parte expositiva: Hellen Rodríguez Loría
Parte dispositiva: Nancy Vílchez Obando
Leído y confrontado: nvo/emr