ASAMBLEA LEGISLATIVA DE LA

REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

REFORMA INTEGRAL A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES

EXPEDIENTE N° 22.388

ENRIQUE SÁNCHEZ CARBALLO

Y OTROS/AS DIPUTADOS/AS

PROYECTO DE LEY

REFORMA INTEGRAL A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES

Expediente N° 22.388

ASAMBLEA LEGISLATIVA:

La “Era de los Datos” plantea un gran reto para los Derechos Humanos así como para los Congresos del mundo entero. La llegada de diversas innovaciones tecnológicas en el análisis, recopilación y procesamiento de datos, así como varias coyunturas globales de reciente data, han puesto en relieve la necesidad de crear marcos normativos mucho más robustos en lo que se refiere al tratamiento de datos personales.

En 2016, Dominic Cummings, director de la campaña *Leave EU* -a favor de la salida de Reino Unido de la Unión Europea-, presentó al hoy Primer Ministro británico, Boris Johnson, una novedosa estrategia para ganar el referéndum conocido como *Brexit*. La estrategia consistía en usar los datos personales que los votantes entregan en sus redes sociales para crear perfiles psicosociales, y con ellos definir mensajes personalizados que permitieran inducir el voto.

Esa propuesta llegó al director de campaña de manos de la empresa AggregateIQ, aliada de la mundialmente conocida Cambridge Analytica (CA). Como se demostró en el Parlamento Británico posteriormente, CA participó en la campaña, y aportó los datos de los votantes y el software que generó los perfiles y la campaña personalizada. Por medio de los perfiles psicosociales, se dividió a los votantes en descartables, seguros, y potenciales. Para este último grupo, se trabajaron mensajes altamente personalizados basados en sus preocupaciones, en gran medida noticias falsas que alimentaban sus temores y desinformación.

Ese software también permitió identificar a aquellas personas desinteresadas en la política: quienes desde hace mucho tiempo no votaban o nunca habían votado en ningún proceso. Miles de estos votantes se encontraban en poblados alejados de los grandes centros de población, habiendo sido excluidos del proceso democrático, y también desplazados por los procesos de gentrificación (Harvey, 2013). Dicho grupo recibió por primera vez en mucho tiempo la visita de políticos que prometían empleo, seguridad social y vivienda... si el Reino Unido abandonaba la Unión

Europea. Ese nivel de precisión -incluso fuera de las redes sociales- permiten las campañas de microtargeting basadas en datos personales.

Cambridge Analytica estuvo en el centro del escándalo desde marzo de 2018, cuando los diarios The Guardian, The New York Times y The Observer, revelaron que la consultora política accedió a los datos personales de 50 millones de usuarios de Facebook sin su autorización, y que fueron usados por la campaña del expresidente de los Estados Unidos, Donald Trump, con una estrategia digital prácticamente idéntica a la ejecutada en el Brexit (Graham y Cadwalladr, 2019). En este caso el énfasis también estuvo en la política migratoria y en divulgar noticias falsas sobre la candidata demócrata, Hillary Clinton.

La revelación la hizo uno de los creadores del sistema, Christopher Wylie, quien relató que los datos surgieron de un test de personalidad desarrollado por el profesor de la Universidad de Cambridge, Aleksandr Kogan, que, como muchas aplicaciones, requería a los usuarios iniciar sesión en Facebook y otorgar algunos permisos de acceso. 270 mil personas hicieron el test, sin saber que al hacerlo estaban autorizando a la aplicación recopilar toda su información y la de todos sus amigos de la red social, sumando alrededor de 87 millones de personas. Tampoco sabían que esa información iba a ser vendida a CA por 800 mil dólares.

El ex empleado de CA también reveló que Facebook supo lo que estaba pasando con los datos de sus usuarios muchos meses antes de que fuera divulgado por los medios de comunicación. Fue hasta después del escándalo, y de que las acciones de la red social tuvieran una millonaria caída, que su fundador y CEO, Mark Zuckerberg, reconoció públicamente los fallos en la seguridad (BBC Mundo, 2018).

Después de diversas investigaciones, Cambridge Analytica cerró, mientras Facebook siguió en el foco de atención por sus problemas de seguridad y el uso de los datos de sus usuarios. Tiempo después, la Comisión Federal de Comercio de Estados Unidos ordenó a la red social a pagar US$5.000 millones como sanción por las malas prácticas en el manejo de la seguridad de los datos de los usuarios. En Reino Unido, la red social fue condenada a pagar una multa de 500.000 libras (US $600.000) ante la Oficina del Comisionado de Información del Reino Unido por el mismo caso. La Resolución del Parlamento Europeo contra Facebook, del 25 de octubre de 2018, confirmó que se utilizaron datos personales de forma irregular por parte de Cambridge Analytica, dentro de los que se encontraban los datos de 2,7 millones de ciudadanos de la Unión.

Una visión de derechos humanos y centrada en las personas

Toda esta coyuntura profundizó las discusiones relacionadas al uso de los datos en el ámbito político-democrático, así como a los cambios que debían realizarse en las legislaciones del mundo. Como es evidente, las redes sociales están en el centro de tales debates.

Ciertamente, cada vez cobra más relevancia este tema entre una mayoría de la población; prueba de ello es la reciente migración masiva de la red de mensajería WhatsApp hacia otros servicios como Signal o Telegram (en el caso de Telegram, llegando a reportar 8 millones de personas usuarias nuevas por día a mediados de enero), debido a cambios en los términos y las condiciones de uso de WhatsApp, vinculados a cómo se usarían los datos y metadatos de sus usuarios (Sanz, 2021).

A pesar de esa creciente conciencia, coyunturas como las de Cambridge Analytica dejan claro que las empresas que lucran con los datos se aprovecharon de varios elementos claves: que las personas usuarias con su "permiso", daban acceso a casi la totalidad de los datos colocados en sus perfiles así como a datos sobre su uso e interacción; que tales permisos acarreaban una falta de control sobre sus datos (una especie de "no retorno") y que esencialmente las personas utilizan dichas redes para generar reacciones (likes) exponiendo su vida personal, y compartiendo información que provoque autosatisfacción, lo que permite conocer con gran precisión el perfil psicológico de esas personas de forma masiva.

"El acto de compartir noticias e información en redes sociales tiene que ver con la emoción que nos genera el contenido y que queremos socializar con el resto de las personas. Así, nos damos cuenta de que las redes sociales más que ser espacios de aislamiento social, son todo lo contrario: una proyección de nosotros mismos y un lugar donde queremos compartir no solo información, sino también emociones" (Valenzuela y Arriagada, 2016).

Este es precisamente el gran valor que hay en en los datos personales en redes sociales: al haber tantísima información, tienen el potencial de identificar muy precisamente las necesidades, los miedos, los intereses de las personas y de incluso predecir los comportamientos, no solo en aspectos eminentemente comerciales o de consumo, sino en términos políticos. "La psicopolítica digital es capaz de llegar a procesos psíquicos de manera prospectiva. Es quizá mucho más rápida que la voluntad libre. Puede adelantarla. La capacidad de prospección de la psicopolítica digital significaría el fin de la libertad" (Hans y Bergés, 2014).

En este sentido, el abordaje de este gran reto debe hacerse desde el enfoque de los derechos humanos y debe comprender el valor que tiene para la robustez de las sociedades democráticas. Los marcos normativos deben tener como prioridad y centro a la persona, de forma que se garantice su autonomía y su autodeterminación alrededor de cómo se usa la información y la data que genera su vida, su interacción social, su interacción digital.

“Estos marcos deben estar centrados en el usuario y enfocarse en amparar y fortalecer los derechos, al tiempo que proporcionen reglas claras y predecibles para que las cumplan las entidades públicas y privadas.” (AccessNow, 2018) Es decir, si bien los casos de mayor conocimiento público global -como los descritos arriba- han estado relacionados a empresas del sector privado, al enfocar la discusión sobre la actualización de la normativa *desde* las personas, les protege también ante los Estados y las instituciones públicas, evitando así usos abusivos de la información y brindando un marco de garantías más firme para la defensa de sus derechos.

“Asimismo, y como se ha podido observar a partir de los escándalos recientes que involucran a empresas del sector privado intensivas en el uso de datos, es necesario evitar que, sin contar con la experiencia necesaria, los gobiernos caigan en la tentación de desarrollar sistemas que utilicen los datos de los ciudadanos sin que incorporen paralelamente un enfoque ético y responsable desde su diseño que asegure cuestiones básicas como la privacidad o el consentimiento. Lo que aquí está en juego no es otra cosa que sentar las bases para un nuevo contrato social que permita una utilización masiva y responsable de los datos por parte de las entidades gubernamentales para proporcionar mejores servicios sociales, al tiempo que se mantiene la confianza de los ciudadanos en que los gobiernos gestionen sus datos de manera responsable.” (BID, 2019)

Datos sin protección: el reto de actualizar la normativa

Si bien ya en la década de los noventa muchos países del mundo contaban con leyes para la protección de los datos personales de sus ciudadanos, esas normativas no contemplaron un contexto como el descrito anteriormente: la era del Big Data y el desarrollo de tecnologías que tienden a que las personas pierdan el control y algunas veces hasta prácticamente la propiedad, sobre sus datos.

Costa Rica, en definitiva, no escapa a este panorama. El país cuenta con una Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales aprobada en 2011 -cuya discusión legislativa se remonta a inicios de los 2000-, que establece regulaciones para el manejo y procesamiento de datos sensibles en las bases de instituciones públicas y empresas, y que fue considerada de avanzada al momento de su creación. Sin embargo, carece de varios conceptos actuales, lo que le da un alcance relativamente limitado para tutelar correctamente los derechos de la ciudadanía en la era de la información y las nuevas tecnologías de recolección y procesamiento de datos.

El informe “Cyber Troops Country Profile: Costa Rica”, de Simone Bunse (2021), ha dejado ver que si bien en la actualidad las tácticas digitales para esparcir desinformación y propaganda electoral carecen de alta sofisticación, el uso de

redes sociales con estos fines se acrecienta, ya se ha probado la contratación y el uso de servicios en el extranjero con estos fines, y es probable que su uso pueda acrecentarse y normalizarse en un futuro no muy lejano.

Por otro lado, también existen falencias y debilidades a nivel institucional -varias de ellas originadas en la ley- que no han permitido a la Autoridad Nacional de Protección de datos, la Prodhab, para hacer cumplir la ley actual y por tanto también deben subsanarse.

El Reglamento General de Protección de Datos de la Unión Europea: un referente global

El derecho a la protección de los datos personales está relacionado con el derecho a la privacidad, pero sus alcances son distintos. Más de 160 países consagran el derecho a la privacidad en sus constituciones, pero el entendimiento de lo que implica varía de un país a otro. Los estados miembros de la Unión Europea representan una excepción en este sentido, ya que reconocieron la protección de datos como un derecho fundamental en la Carta de 2001 de la UE.

La normativa que ha desarrollado la Unión Europea en materia de protección de datos ha servido de referente en para el resto del mundo, aunque ciertamente desde su aprobación también se han encontrado diversas oportunidades de mejora. En 2016, entró en vigor el Reglamento General de Protección de Datos (RGPD) y fue de aplicación en 2018. Una de sus virtudes fue el desarrollo de principios claros bajo los cuales debe realizarse cualquier tratamiento de datos personales, comprendiendo así que más allá de la tecnología utilizada o los términos en que se acordó el tratamiento de los datos en particular, los fundamentos desde los que se realiza dicho tratamiento deberían ser siempre la mismos.

Principio	**Resumen**
Limitación del fin	El tratamiento debe estar limitado a los fines legítimos para los cuales los datos personales fueron recogidos originalmente.
Minimización de datos	Al momento de recoger datos, sólo se pueden solicitar los datos personales absolutamente necesarios para el fin legítimo acordado con la persona titular.

Exactitud	Los datos personales de los interesados deben ser siempre precisos y estar actualizados.
Integridad y confidencialidad	Los datos personales deben ser tratados de forma que se garantice la seguridad apropiada, incluyendo protección contra el tratamiento no autorizado o ilegal.
Limitación del almacenamiento	Los datos solo deben ser conservados mientras sea necesario. Es decir, deben de ser eliminados una vez se haya cumplido el fin legítimo para se recogieron.
Lealtad y transparencia	Las empresas no deben realizar tratamientos que no sean legítimos, es decir, deben ser leales hacia las personas titulares con respecto a la ley. Además, las empresas deben ser transparentes con respecto al tratamiento, e informar a la persona interesada de manera abierta y transparente.

Cuadro 1. Principios para el tratamiento de datos personales en el RGPD. Basado en el RGPD de la Unión Europea y Bhatia, P. (2018).

Asimismo, otro de los desarrollos conceptualmente interesantes del RGPD fueron las categorías de derechos, los cuales se plantearon bajo el mismo paradigma de procurar que, más allá de una tecnología o tipo de uso concreto, las personas usuarias puedan ejercer esos derechos en toda circunstancia, de manera que, además de ser derechos vinculantes para todo tratamiento de datos personales, deben ser de acceso gratuito y de aplicación permanente.

Derecho	**Resumen**
Derecho de acceso	Habilita a los usuarios a obtener confirmación de los servicios y compañías con respecto a la posible recopilación y procesamiento de sus datos personales. Los usuarios deben tener acceso a los datos y el propósito del procesamiento.
Derecho de oposición	Permite a los usuarios a rehusarse al procesamiento de su información personal cuando no hayan prestado su consentimiento o no hayan firmado un contrato.

Derecho de supresión	Permite que los usuarios soliciten la eliminación de todos sus datos personales cuando dejan un servicio o aplicación.
Derecho de rectificación	Permite que los usuarios soliciten la modificación de información errónea.
Derecho a la información	Garantiza que los usuarios reciban información clara y entendible por parte de las entidades que procesan sus datos, ya sea que estas entidades los recopilaron de manera directa o a través de terceros. Toda la información provista al usuario debe ser concisa, comprensible, y de fácil acceso.
Derecho a la explicación	Motiva a los usuarios a obtener información sobre el tratamiento de datos personales automatizado y sus consecuencias. Este derecho es esencial para conocer el uso de algoritmos que tienen un impacto en la vida de los usuarios.
Derecho a la portabilidad	Permite que los usuarios movilicen datos personales que han compartido de una plataforma a otra que ofrezca servicios similares.

Cuadro 2. Derechos para el tratamiento de datos personales en el RGPD. Basado en el RGPD de la Unión Europea.

La lista, que no es exhaustiva, permite ver las diversas dimensiones en que debe tutelarse la autodeterminación informativa de la ciudadanía y, además que estamos ante un ámbito que requiere de mucha precisión y visión al confeccionar normativa, al tratarse de conceptos jurídicos que aplican a situaciones altamente cambiantes, con muchas posibles vulnerabilidades para la integridad de las personas.

Legislación consultada sobre protección de datos personales

Como parte de la construcción de esta propuesta, se analizaron diferentes legislaciones, junto al RGPD, para incorporar otros aspectos en que había oportunidades de mejora. Entre las legislaciones consultadas están las siguientes:

Jurisdicción	**Nombre de la norma**	**Año**
Argentina	Proyecto de Ley de Protección de Datos Personales	Presentación: 2017

Brasil	Ley General de Protección de Datos Personales (LGPD)	Aprobación: 2018 Vigencia: 2020
Canadá	Proyecto de Reforma a la Ley de Privacidad (Privacy Act)	Presentación: 2020
Nueva Zelanda	Privacy Act	Vigencia: 2020
Ecuador	Proyecto de Ley Orgánica de Protección de Datos	Presentación: 2019
Estado de California, Estados Unidos	Ley de Privacidad para el Consumidor del Estado de California	Vigencia: 2018
Estado de California, Estados Unidos	Ley de Derechos de Privacidad del EStado de California	Vigencia: 2020
Unión Europea (Parlamento y Consejo Europeo)	Reglamento General de Protección de Datos	Aprobación: 2016 Vigencia: 2018

Protección de Datos en América Latina

En cuanto a la legislación consultada en América Latina, conviene destacar, una legislación de reciente aprobación, la Ley General de Protección de Datos Personales de Brasil (LGPD), que entró en vigor en 2020, después de su aprobación en 2018 y dos años de vacancia. Si bien en términos de los principios y derechos que se explicaron, así como sus sanciones, usa un marco similar al RGPD, se encuentran algunas diferencias que son interesantes de destacar:

- Incorporó medidas mucho más restrictivas para el tratamiento de datos de personas menores de edad, en particular para la obtención del consentimiento informado. La edad debajo de la cual aplican estas restricciones son los 18 años (en el RGPD, esto es hasta los 16) y la información que recibe la persona titular tiene requisitos más específicos sobre su claridad, explicación del tratamiento, e inclusive el formato.

- Las sanciones a empresas fueron relativizadas al contexto brasileño, reduciendo los porcentajes a 2% de la facturación, mientras que en el RGPD este porcentaje llega hasta a 8% en algunos casos.

- En el tema de notificación de brechas de seguridad, la LGPD tiene plazos de notificación menos severos y específicos que el RGPD.

- En el tema de transferencia transfronteriza de datos, disminuyó las excepciones con las que cuenta el RGPD para validar la transferencia de un tercer país a la jurisdicción brasileña, dando como resultado un marco más estricto.

Este marco jurídico de protección de datos personales se considera uno de los más de avanzada en la región, siendo que cumple con los estándares más innovadores e incorpora temas novedosos, como el marco de protección de derechos de personas menores de edad y se adapta a la realidad jurídica e institucional brasileña.

Sin haber conseguido su aprobación aún, existen otros esfuerzos en América Latina orientados a actualizar las normas a estándares más innovadores de protección de datos personales. Uno de ellos es el proyecto de ley de protección de datos en Argentina, que, a grandes rasgos, utiliza la base de principios (en su capítulo 2) y derechos (en su capítulo 3) del RGPD de la UE. La iniciativa presentaba puntos de discusión álgidos como las excepciones al consentimiento por motivaciones de "seguridad nacional" muy abiertas o justificaciones difusas para evitar notificar a las personas usuarias sobre el tratamiento de sus datos, así como la poca independencia que tendría la autoridad de control de protección de datos personales (Pisanu, 2018), sin embargo, se ha procurado corregirlas en versiones recientes del proyecto de Ley.

Otro proyecto que resulta de interés mencionar es el Proyecto de Ley de Orgánica de Protección de datos personales del Ecuador, que tiene como fin adecuar sus normas a los estándares europeos, motivados también por aspectos de comercio internacional, siendo que dicho país actualmente no cuenta con un marco regulatorio específico para la Protección de Datos Personales: "al no tener normativa amparada por un ente controlador especializado en la materia, no le es posible al país ofrecer un nivel adecuado de protección, lo que desalienta el comercio y genera que se prefieran destinos como Colombia, Perú y los demás países suscriptores del acuerdo, que sí cuentan con Ley de Protección de Datos Personales".

La orientación hacia la persona usuaria del proyecto de ley se puede observar en los principios que rigen el tratamiento (Capítulo II), los derechos que le asisten a las personas titulares de los datos (Capítulo III) y la especificidad de las normas de garantías para la seguridad y el tratamiento de los datos, así como las exigencias de responsabilidad proactiva que exigiría a las empresas y entidades que realicen algún tipo de tratamiento de datos personales.

Estas son legislaciones e iniciativas de la región que buscan ubicarse a la vanguardia de los estándares de protección de datos a nivel global, partiendo de los principios y derechos protegidos por la normativa europea, pero adaptándola a los contextos latinoamericanos y solventando oportunidades de mejora detectadas en el propio RGPD. Es en esta línea que se ha trabajado la presente propuesta legislativa.

La ley 8968: ¿cuáles son sus áreas de mejora?

Como se ha señalado, la Ley de Protección de Datos Personales que esta propuesta pretende remozar fue una legislación de avanzada en el momento de su aprobación, en 2011. Sin embargo, las primeras discusiones legislativas (que dan base a dicha legislación) datan de 2003. Esto, sumado al vertiginoso cambio tecnológico alrededor del tratamiento de datos personales -el cual hemos buscado sintetizar a lo largo de esta exposición de motivos-, definitivamente ha modificado las bases sobre las cuales una legislación robusta debería estar asentada.

Partiendo del contexto descrito, los referentes que se han analizado y la realidad institucional y nacional sobre protección de datos personales, se recogen a continuación los principales aspectos en los que se considera que la legislación costarricense tiene oportunidades de mejora.

1) **Actualización de conceptos base utilizados en la legislación.** Las nociones básicas a las cuales hace referencia la Ley vigente han sido superados en muchos casos. En algunas ocasiones, esto implicaría remozar conceptos ya empleados; en otras, añadir concepciones inexistentes en la legislación. Buenos ejemplos de esto son conceptos como “datos biométricos”, “datos genéticos” o “seudonimización”.

2) **Desarrollo de los principios que rigen el tratamiento de datos personales, así como de los derechos que le asisten a las personas titulares.** Teniendo como referente el RGPD de la Unión Europea, es evidente que los principios explicitados en la Ley Nº 8968 son limitados y no generan un marco robusto para el tratamiento de datos en el país. Principios como la lealtad, la transparencia, la minimización de datos o la finalidad o conservación limitada son ejemplos de ello. Asimismo, los derechos que le asisten a la persona tienen múltiples áreas de mejora, en casos como el derecho de oposición, limitación del tratamiento, supresión, o la portabilidad.

3) **Limitación tajante de las excepciones a la autodeterminación informativa de la persona interesada, y clarificación de las excepciones al consentimiento informado.** Una de las áreas más relevantes de mejorar. Las excepciones a la autodeterminación informativa en la Ley vigente son excesivamente amplias y riesgosas para la ciudadanía, pues abren muchísimas posibilidades de disminuir la totalidad de garantías (y no solo el consentimiento informado) establecidas en la Ley, lo cual es urgente de limitar únicamente a casos determinados por Ley o por vía judicial. Por otro lado, las excepciones al consentimiento informado de la persona interesada,

deben ser clarificados y establecidos de manera específica, cerrando el lugar a interpretación en la normativa.

4) **Fortalecimiento institucional de la Autoridad Nacional, la Prodhab.** Este fortalecimiento va en dos sentidos: a) Dotar de independencia de criterio al órgano, mediante su traslado a un ámbito de la administración pública menos sujeta a determinaciones políticas coyunturales y b) Robustecer presupuestariamente a la Prodhab a través de nuevos mecanismos de ingreso y una mayor flexibilidad en el uso de los recursos recaudados por cánones y multas.
5) **Fortalecimiento de las garantías para la seguridad y la confidencialidad.** Implementar nuevas y mejores medidas preventivas, especialmente para tratamientos de datos de mayor riesgo. Entre los mecanismos que se podrían utilizar están robustecer los protocolos de actuación, los estudios de impacto o el requerimiento de una persona delegada de datos.
6) **Fortalecimiento del esquema de sanciones.** Actualización del esquema de sanciones de manera que esté acorde con la realidad económica del mercado de datos en la actualidad, bajo la premisa de que no sea más "rentable" para un ente responsable de tratamiento de datos, pagar multas que cumplir la ley.
7) **Desarrollo de bases claras para la transferencia transfronteriza de datos.** Establecer reglas nuevas bajo las cuales la Autoridad Nacional pueda determinar cuando es posible y válido realizar una transferencia de datos a otra jurisdicción, resguardando la integridad de los datos de las personas titulares de los mismos.

Respondiendo a las consideraciones de fortalecimiento de la Ley Nº 8968, Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales arriba detalladas y con base en las consideraciones previamente expuestas, sometemos a su consideración la presente iniciativa de ley.

Bibliografía

AccessNow.org. (2018). La Creación de un Marco para la Protección de Datos: una guía para los Legisladores sobre qué hacer y qué no. https://www.accessnow.org/cms/assets/uploads/2018/04/manual-de-proteccion-de-datos.pdf

BBC Mundo. (2018, 21 marzo). Cambridge Analytica: Mark Zuckerberg reconoce que Facebook cometió errores en medio del peor escándalo que ha enfrentado la red social. de https://www.bbc.com/mundo/noticias-43484188

Bunse, S. (2021) Global Cyber Troops Country Profile: Costa Rica. LEAD University & Georgetown University. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/Cyber-Troop-Costa-Rica-2020.pdf

Banco Interamericano de Desarrollo, BID. (2019). LA GESTIÓN ÉTICA DE LOS DATOS: Por qué importa y cómo hacer un uso justo de los datos en un mundo digital. https://publications.iadb.org/publications/spanish/document/La_Gesti%C3%B3n_%C3%89tica_de_los_Datos.pdf

Hans, B. C., & Bergés, A. (2014). Psicopolítica: neoliberalismo y nuevas técnicas de poder. Barcelona, España: Herder.

Harvey, D. (2013). Ciudades rebeldes. Tres Cantos: Akal.

Graham-Harrison, E., & Cadwalladr, C. (2019, 21 junio). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Presidência da República, Brasil. (2019). Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Valenzuela, S. & Arriagada, A. (2016). Viralizando la emoción y por qué la compartimos online. En A. Arriagada (ed.). El mundo en mi mano: La revolución de los datos móviles. Santiago: Fundación País Digital.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

DECRETA:

REFORMA INTEGRAL A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES

ARTÍCULO ÚNICO- Se reforma integralmente la Ley N° 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales del 5 de setiembre de 2011, que en lo sucesivo dirá:

"LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES

CAPÍTULO I

DISPOSICIONES GENERALES

SECCIÓN ÚNICA

ARTÍCULO 1.- Objetivo y fin

Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su autonomía personal con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona.

ARTÍCULO 2.- Ámbito de aplicación material

Esta ley será de aplicación al tratamiento de los datos personales, incluyendo la recopilación, el uso, la retención y análisis, por organismos públicos o privados.

El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas, siempre y cuando estas sean utilizadas con fines exclusivamente personales o domésticos y no sean vendidas o de cualquier otra manera comercializadas, incluyendo fines de prospección.

ARTÍCULO 3.- Ámbito de aplicación territorial

Esta ley se aplica en cualquiera de las siguientes circunstancias:

a) Cuando haya tratamiento de datos personales recopilados en territorio costarricense en el contexto de las actividades propias del responsable de la base de datos, independientemente de que dicho tratamiento tenga lugar en Costa Rica o no.

b) Cuando haya tratamiento de datos de personas que residan en la República de Costa Rica por parte de un responsable no establecido en el territorio costarricense, independientemente de si a las personas interesadas se les requiere su pago o no.

ARTÍCULO 4.- Definiciones

Para los efectos de la presente ley se define lo siguiente:

a) **Base de datos:** cualquier clase de fichero, que sea objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

b) **Datos personales:** toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

c) **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.

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

e) **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;

f) **Fuentes de acceso público:** Bases de datos que pueden ser consultadas por cualquier persona física o jurídica, pública o privada, nacional o internacional cuyo acceso no se encuentre limitado por la normativa vigente o disposición de la Autoridad de Protección de Datos Personales

g) **Datos sensibles:** Datos relativos a etnia, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, identidad de género, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas. Los metadatos que identifiquen o hagan identificable a un ser humano, también formarán parte de este concepto, en la medida en que puedan dar origen a discriminaciones o vulneraciones de derechos humanos, y estarán definidos vía reglamentaria. Igualmente, por vía reglamentaria, la Autoridad de Protección de Datos Personales podrá determinar otras categorías de datos sensibles que no estén expresamente enumeradas en el listado de este inciso.

h) **Datos de acceso restringido:** todos los datos personales privados que no se consideren sensibles. Son de interés únicamente para su titular o para la Administración Pública. No son de acceso irrestricto independientemente de si forman o no parte de fuentes de acceso público o se encuentran en bases de datos de la Administración Pública.

i) **Datos de acceso irrestricto:** datos de acceso general, contenidos en bases de datos públicas, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

j) **Deber de confidencialidad:** obligación de los responsables del tratamiento de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (Prodhab), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente

cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aún después de finalizada la relación con la base de datos.

k) **Encargado:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

l) **Fichero:** todo conjunto estructurado de datos personales, manual o automatizado, accesible con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

m) **Persona interesada:** persona física titular de los datos que sean objeto del tratamiento, total o parcialmente automatizado o manual.

n) **Responsable:** persona física o jurídica, sea pública o privada, que administre, gerencie o se encargue de una base de datos, quién es competente para señalar, con arreglo a la ley, cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento se les aplicarán.

o) **Seudonimización**: Tratamiento de datos personales de manera tal que ya no puedan atribuirse a la persona interesada 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.

p) **Tratamiento o procesamiento de datos personales:** cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos total o parcialmente automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

q) **Grupo de interés económico:** agrupación de sociedades que se manifiesta mediante una unidad de decisión, es decir, la reunión de todos los elementos de mando o dirección empresarial por medio de un centro de operaciones, y se exterioriza mediante dos movimientos básicos: el criterio de unidad de dirección, ya sea por subordinación o por colaboración entre empresas, o el criterio de dependencia económica de las sociedades que se agrupan, sin importar que la personalidad jurídica de las sociedades se vea afectada, o que su patrimonio sea objeto de transferencia, independientemente de su

domicilio y razón social. Cuando la PRODHAB lo requiera la condición de grupo de interés económico podrá ser demostrada por medio de una declaración jurada protocolizada o documento legal equivalente de la jurisdicción del titular de la base de datos sin perjuicio de las facultades de investigación de la PRODHAB.

CAPÍTULO II

PRINCIPIOS Y DERECHOS PARA LA PROTECCIÓN DE DATOS PERSONALES

SECCIÓN I

PRINCIPIOS QUE RIGEN EL TRATAMIENTO DE DATOS PERSONALES

ARTÍCULO 5.- Principio de lealtad y legalidad

Los datos personales deben ser procesados de manera justa y en apego a los límites de esta ley y el marco normativo vigente. Toda información deberá ser procesada con una base jurídica lícita, con un propósito definido, y de una manera justa y transparente. Las personas usuarias deberán ser informadas pertinentemente sobre cómo se recopilarán, usarán o almacenarán sus datos y quién lo hará.

ARTÍCULO 6- Principio de transparencia de la información

El responsable del tratamiento tomará las medidas oportunas para facilitar a la persona interesada todas las informaciones indicadas en esta Ley, así como cualquier comunicación relativa al tratamiento de datos personales, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a la población infantil. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite la persona interesada, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

ARTÍCULO 7.- Principio de finalidad y conservación limitadas

Los datos personales deberán ser recopilados y procesados sólo para fines determinados, explícitos y legítimos. El propósito para el que se procesan dichos datos debe ser explícito y no deberán ser conservados por más tiempo que el

necesario para cumplir con ese fin. Los datos no deben ser procesados de una manera que sea incompatible con dicho propósito.

No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley.

ARTÍCULO 8.- Principio de minimización de datos

Los datos personales procesados y recopilados deben limitarse a ser suficientes, pertinentes y no excesivos en relación con el propósito específico y definido previamente.

ARTÍCULO 9.- Principio de calidad de la información

Solo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento total o parcialmente automatizado o manual, cuando tales datos sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados. Los usuarios deben tener el derecho a eliminar, rectificar, y corregir su información personal, la cual debe cumplir con las siguientes características:

a) **Actualidad:** Los datos de carácter personal deberán ser actuales. El responsable de las bases de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular.

b) **Veracidad:** Los datos de carácter personal deberán ser veraces. La persona responsable de la base de datos está obligada a modificar o suprimir los datos que falten a la verdad.

c) **Exactitud:** Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos -del todo o en parte- o incompletos sean suprimidos de la base de datos o sustituidos por los correspondientes datos rectificados, actualizados o complementados, respetando los fines para los que fueron recogidos o tratados.

ARTÍCULO 10.- Principio de integridad y confidencialidad

Los datos personales deben ser procesados de manera que se garantice la seguridad e indemnidad de los mismos, así como la protección contra el tratamiento no autorizado o ilegítimo y contra la pérdida accidental, destrucción o daños de los

datos. Para todo ello, se tomarán las medidas técnicas y organizacionales pertinentes que eviten vulnerabilidades en el acceso a dicha información.

ARTÍCULO 11.- Principio de gratuidad

Se establece el principio de gratuidad en el ejercicio de los derechos tutelados por la presente ley, para la persona que posea la titularidad de los datos personales o en el caso de la persona menor de edad, para su representante legal.

SECCIÓN II

DERECHOS DE LA PERSONA ANTE EL TRATAMIENTO DE SUS DATOS PERSONALES

ARTÍCULO 12.- Autodeterminación informativa

Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta ley.

Se reconoce la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones y datos concernientes a cada persona, cuya titularidad sobre los datos es exclusiva e irrenunciable. Este derecho es la manifestación de la protección a la intimidad, en el ámbito del tratamiento de datos personales, evitando que se propicien acciones discriminatorias o usos inadecuados de los mismos.

ARTÍCULO 13.- Consentimiento informado

Cuando se soliciten datos de carácter personal, la persona titular de los datos tiene derecho a ser informada de modo expreso, preciso e inequívoco de la posible recopilación y procesamiento de sus datos personales, como mínimo sobre los siguientes aspectos:

a) La existencia de una base de datos personales.

b) Las categorías de datos personales contenidas en la base.

c) Los fines que se persiguen con la recolección de estos datos y la base jurídica del tratamiento.

d) Los destinatarios de la información, así como de quiénes podrán consultarla.

e) El carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos.

f) El tratamiento que se dará a los datos solicitados.

g) Las consecuencias de la negativa a suministrar los datos.

h) La posibilidad de ejercer los derechos que le asisten.

i) La identidad y datos de contacto del responsable de la base de datos.

j) El plazo durante el cual se conservarán los datos personales.

k) El derecho a presentar una reclamación ante las autoridades correspondientes.

l) La existencia o no de decisiones automatizadas, incluida la elaboración de perfiles.

Cuando se utilicen cuestionarios u otros medios para la recolección de datos personales figurarán estas advertencias en forma claramente legible. No obstante, dependiendo del mecanismo utilizado para la recolección del Consentimiento Informado, la Autoridad de Protección de Datos Personales podrá autorizar formas simplificadas respecto de los contenidos de los aspectos señalados, siempre cuando la información quede a disposición del interesado, en el momento que éste haga requerimiento de la misma.

ARTÍCULO 14.- Otorgamiento del consentimiento

Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar en forma expresa, ya sea en un medio físico o electrónico. El consentimiento podrá ser revocado en cualquier momento, sin efecto retroactivo.

ARTÍCULO 15.- Excepciones al consentimiento informado

No será necesario el consentimiento expreso:

a) Cuando así lo disponga o habilite una norma de rango constitucional o legal, salvaguardando la integridad de los datos y restringiendo su uso estricto a los fines que persiga dicha norma.

b) Cuando exista orden fundamentada, dictada por autoridad judicial competente.

c) Para la prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones.

d) Para el funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, o para la adecuada prestación de servicios públicos, siempre que los datos se hayan anonimizado previamente y no exista riesgo de que las personas sean identificadas.

e) Cuando el tratamiento sea necesario para la ejecución de un contrato solicitado por la persona titular. O bien, para la aplicación de un contrato en el que el interesado es parte.

f) Cuando es necesario el tratamiento para proteger intereses vitales de la persona interesada o de otra persona física, si la persona interesada no está capacitada, física o jurídicamente, para dar su consentimiento.

g) Cuando el tratamiento es necesario para el cumplimiento de una finalidad realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Se prohíbe en todo caso el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos.

ARTICULO 16. - Condiciones aplicables al consentimiento de la persona menor de edad en relación con los servicios de la sociedad de la información

Cuando se apliquen los principios relativos al consentimiento informado en relación con la oferta directa a personas menores de edad de servicios de la sociedad de la información, el tratamiento de los datos personales de una persona menor de edad se considerará lícito cuando tenga como mínimo 15 años. Si es menor de 15 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo autorizó el titular de la patria potestad o tutela sobre el niño o la niña, y solo en la medida en que se dio o autorizó.

El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño o la niña, teniendo en cuenta la tecnología disponible.

ARTÍCULO 17.- Excepciones a la Autodeterminación Informativa

Los derechos y las garantías establecidos en esta ley podrán ser limitados en las siguientes circunstancias:

a) Cuando así lo disponga o habilite una norma de rango constitucional o legal, salvaguardando la integridad de los datos y restringiendo su uso estricto a los fines que persiga dicha norma.

b) Cuando exista orden fundamentada, dictada por autoridad judicial competente.

ARTÍCULO 18.- Derecho de acceso a los datos personales

Las personas usuarias deberán tener derecho de acceso a los datos recopilados, el propósito del procesamiento y a conocer quiénes los procesarán en cualquier momento. La información deberá ser almacenada en forma tal que se garantice plenamente el derecho de acceso por la persona interesada.

La persona responsable del tratamiento de los datos debe facilitar la información que la persona solicite, de manera gratuita, y resolver en el sentido que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud. Las entidades deben brindar su información de contacto y una dirección de correo electrónico a las personas usuarias para que estas puedan comunicarse con ellos en caso de que existan problemas.

El derecho de acceso a la información personal garantiza las siguientes facultades de la persona interesada:

a) Obtener en intervalos razonables, según se disponga por reglamento, sin demora y a título gratuito, lo siguiente: confirmación o no de la existencia de datos suyos en archivos o bases de datos, el propósito por el que se procesan, destinatarios o personas autorizadas, origen de la recolección de datos, categoría de datos procesados, plazo previsto de conservación, si los datos están siendo utilizados para la toma de decisiones automáticas o si los mismos están siendo transmitidos a terceros países.

b) En caso de que existan datos o información relativa a su persona, estos le deberán ser comunicados y brindados en forma precisa, entendible, de fácil acceso y con lenguaje simple y claro. Además, la persona interesada también podrá saber la finalidad con que fueron recopilados los datos y el uso que se les ha dado, bien hayan sido recopilados de manera directa o a través de terceros. El informe deberá ser completo y exento de codificaciones. Deberá estar acompañado de una aclaración de los términos técnicos que se utilicen.

c) Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes

a terceros, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.

El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, le corresponderá a sus sucesores o herederos.

ARTÍCULO 19.- Derecho a la explicación

Las personas interesadas tienen derecho a una explicación sobre las lógicas y mecanismos empleados, además de los fines y las consecuencias, para el procesamiento automatizado de los datos personales que hayan sido recopilados. Dentro de esta explicación estará incluido todo algoritmo cuyo diseño o programación pueda tener un impacto en el destino o uso de los datos recopilados, y de ser solicitado será incluido dentro de los reportes requeridos por las personas usuarias sobre el tratamiento de sus datos.

ARTÍCULO 20.- Derecho de oposición

La persona usuaria podrá oponerse al procesamiento de sus datos personales, si no ha mediado su consentimiento para ello, o no lo ha expresado o aceptado por escrito de forma física o digital. En cualquier momento, el titular de los datos personales puede oponerse a la utilización de sus datos para la toma de decisiones automáticas, parcialmente automáticas o fines de mercadotecnia directa, incluido el análisis de perfiles.

Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, con la excepciones que por efecto de esta ley resulten de aplicación.

ARTÍCULO 21. - Derecho a la limitación del tratamiento

La persona interesada podrá solicitar del responsable la suspensión de todo tratamiento de sus datos personales, reservando los mismos en el estado que se encontraban al momento de surgir los hechos objeto de la solicitud, cuando se cumpla alguna de las siguientes condiciones:

a) La persona interesada impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.

b) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.

c) El responsable ya no necesita los datos personales para los fines del tratamiento, pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

ARTÍCULO 22.- Derecho de rectificación

La persona interesada tendrá el derecho de obtener la rectificación o actualización de sus datos personales, cuando los datos en poder del responsable del tratamiento estén incompletos, desactualizados o sean inexactos.

Dicha rectificación o actualización puede ser solicitada en cualquier momento por la persona titular de los datos, o por la persona encargada legal en el caso de las personas menores de edad, o las personas sin capacidad volitiva o cognoscitiva. En el caso de datos de personas fallecidas, les corresponderá este derecho a sus sucesores o herederos.

ARTÍCULO 23.- Derecho de supresión

La persona interesada tiene derecho a la supresión de sus datos y cualquier información vinculada a su persona al momento en que suspenda el uso de un servicio o aplicación que haya originado la recopilación de los datos. El responsable del tratamiento deberá garantizar la confidencialidad respecto a esa información posterior a la eliminación. Igual derecho tendrá, cuando hayan sido recopilados sin su autorización.

El derecho de supresión no podrá ser ejercido cuando el tratamiento de los datos sea necesario para ejercer el derecho a la libertad de expresión, la libertad de prensa e información, lo cual incluye las expresiones periodísticas, académicas, artísticas o literarias, de archivo o de investigación científica.

Dicha supresión puede ser solicitada por la persona titular de los datos, o por la persona encargada legal en el caso de las personas menores de edad, o sin capacidad volitiva o cognoscitiva. En el caso de datos de personas fallecidas, les corresponderá este derecho a sus sucesores o herederos.

Igualmente, la persona interesada podrá solicitar la supresión de sus datos personales, cuando medie y legalmente proceda, el retiro del consentimiento informado otorgado al efecto del tratamiento.

ARTÍCULO 24.- Derecho a la portabilidad

Las personas titulares de los datos podrán solicitar el traslado de sus datos personales, o parte de ellos, hacia la base de otra empresa, plataforma o ente

prestador de servicios cuando sea técnicamente posible, posibilidad que determinará la autoridad competente. Para ello se deberán salvaguardar los principios y derechos reconocidos en esta ley.

ARTÍCULO 25.- Autorización para la transferencia de datos

Los responsables de las bases de datos, públicas o privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley.

SECCIÓN III

CATEGORÍAS PARTICULARES DE DATOS PERSONALES

ARTÍCULO 26.- Prohibición del tratamiento de datos sensibles

Queda prohibido el tratamiento de datos personales 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, datos relativos a la salud o datos relativos a la vida sexual de una persona física o cualquier otro dato sensible.

ARTÍCULO 27.- Circunstancias de no aplicabilidad de la prohibición de tratamiento de datos sensibles

El artículo anterior no será de aplicación cuando concurra una de las circunstancias siguientes:

a) El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando en la legislación costarricense se establezca que la prohibición mencionada no puede ser levantada por el interesado;

b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral, de la seguridad social o ayudas sociales, en la medida en que así lo autorice el marco normativo costarricense y establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) El tratamiento es 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 interesados;

e) 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;

f) El tratamiento es necesario 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, en virtud de un contrato con un profesional sanitario;

g) El tratamiento es necesario 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, sobre la base de la legislación costarricense, que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

h) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, 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 interesado.

ARTÍCULO 28.- Datos personales de acceso restringido

Los datos de acceso restringido son todos aquellos datos personales de índole privado que no sean considerados sensibles. Son susceptibles de ser tratados en los términos que esta ley especifica. Si bien estos datos podrían formar parte de bases datos de la Administración Pública o de fuentes de acceso público, no por

ello son considerados de acceso irrestricto, debido a que son de interés únicamente para su titular o para la Administración Pública.

SECCIÓN IV
SEGURIDAD Y CONFIDENCIALIDAD DEL TRATAMIENTO DE LOS DATOS

ARTÍCULO 29.- Seguridad de los datos por diseño y por defecto

La persona responsable de la base de datos deberá adoptar las políticas internas y tomar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cumplir con los principios de esta ley y evitar cualquier acción contraria a la misma.

Dichas políticas y medidas se tomarán desde el diseño y el desarrollo de cualquier aplicación, servicio o producto basado en el tratamiento de datos personales o que tratan datos personales para cumplir su función, y deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual para garantizar la protección de la información almacenada.

Además, deberán reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento y permitir a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad.

No se registrarán datos personales en bases que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas. Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos. Estos principios se tendrán en cuenta para el tratamiento de datos tanto a nivel privado como público, sea o no con fines de lucro.

ARTÍCULO 30.- Deber de confidencialidad

La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser

relevada del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce.

ARTÍCULO 31.- Estudios de impacto

Para aquellas operaciones de tratamiento de datos que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional, que podrían afectar a un gran número de interesados o podrían entrañar un alto riesgo, sea por su alcance, por la sensibilidad de los datos a tratar o por la dificultad para los interesados de hacer cumplir sus derechos, deberá realizarse previamente un estudio de impacto del tratamiento de datos por parte de la persona responsable del tratamiento.

El estudio de impacto deberá valorar la probabilidad y alcance de los riesgos, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Además debe incluir las medidas, garantías y mecanismos previstos para mitigar dichos riesgos, garantizar la protección de los datos personales y demostrar la conformidad con la presente ley.

Las características específicas de dichos estudios serán determinadas vía reglamento. La Autoridad de Protección de Datos determinará cuáles operaciones de tratamiento de datos requerirán dichos estudios al momento de su registro.

ARTÍCULO 32.- Protocolos de actuación

Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, deberán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley.

Los protocolos de actuación deberán ser inscritos, así como sus posteriores modificaciones, ante la Prodhab. La Prodhab podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de su protocolo.

La manipulación de datos con base en un protocolo de actuación inscrito ante la Prodhab hará presumir, “iuris tantum”, el cumplimiento de las disposiciones contenidas en esta ley, para los efectos de autorizar la cesión de los datos contenidos en una base.

ARTÍCULO 33.- Vulneración de Datos Personales.

El responsable deberá informar tanto al titular como a la PRODHAB, sobre cualquier irregularidad en el tratamiento o almacenamiento de sus datos, pérdida de los mismos, destrucción, extravío, alteración o similares, como consecuencia de una vulnerabilidad de la seguridad de la cual entrará en conocimiento, para lo cual tendrá cinco días hábiles a partir del momento en que se conoció la vulnerabilidad, a fin de que los titulares de estos datos personales afectados puedan tomar las medidas correspondientes.

La información mínima que deberá proveerse será:

a) La naturaleza del incidente;

b) Los datos personales comprometidos;

c) Las acciones correctivas realizadas de forma inmediata y las que serán tomadas;

d) Los medios o el lugar, donde puede obtener más información al respecto.

ARTÍCULO 34.- Persona Delegada de Protección de Datos

Si la Autoridad de Protección de Datos determina que la operación de tratamiento presenta altos riesgos para la integridad de los datos personales, el responsable del tratamiento deberá designar a una persona delegada de protección de datos. Dicha persona delegada velará por el cumplimiento legal de la normativa atinente y deberá contar con capacidades y competencias profesionales para responder ante las autoridades. El rol podrá ser asumido por una persona a lo interno de la institución u organización, o por un tercero.

Reglamentariamente se establecerán los requisitos para las personas delegadas, así como los criterios para definir en qué operaciones de tratamiento será necesaria su existencia.

ARTÍCULO 35.- Códigos de conducta

La Agencia de Protección de Datos de los Habitantes, el gobierno central, las instituciones públicas, entes gremiales, asociaciones y empresas privadas, deberán promover la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación de la presente Ley, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas, las pequeñas y medianas empresas.

ARTÍCULO 36.- Garantías efectivas

Toda persona interesada tiene derecho a un procedimiento administrativo sencillo y rápido ante la Prodhab, con el fin de ser protegido contra actos que violen sus derechos fundamentales reconocidos por esta ley. Lo anterior sin perjuicio de las garantías jurisdiccionales generales o específicas que la ley establezca para este mismo fin.

CAPÍTULO III

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES (PRODHAB)

SECCIÓN I

DISPOSICIONES GENERALES

ARTÍCULO 37.- Agencia de Protección de Datos de los Habitantes (Prodhab)

Se crea la Agencia de Protección de Datos de los Habitantes (PRODHAB), como un órgano adscrito al Poder Legislativo de la República y que desempeñará sus funciones con absoluta independencia funcional, administrativa, técnica, presupuestaria y de criterio. Tendrá personalidad jurídica propia en el desempeño de las funciones que le asigna esta ley.

ARTÍCULO 38.- Atribuciones

Son atribuciones de la Prodhab, además de las otras que le impongan esta u otras normas, las siguientes:

a) Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.

b) Llevar un registro de las bases de datos reguladas por esta ley.

c) Requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo.

d) Acceder a las bases de datos reguladas por esta ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y cuando se tenga evidencia de un mal manejo generalizado de la

base de datos o sistema de información y, para la realización de investigaciones sobre la aplicación de la presente ley.

e) Resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales.

f) Ordenar, de oficio o a petición de parte, el acceso, rectificación, supresión, explicación, portabilidad, olvido u oposición, en el tratamiento de las informaciones contenidas en los archivos y las bases de datos, cuando éstas contravengan las normas sobre protección de los datos personales.

g) Imponer las sanciones establecidas, en esta ley, a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de las que puedan configurar delito.

h) Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.

i) Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.

j) Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.

k) Brindar asesoría, capacitación técnica y certificaciones en materia de privacidad, manejo de bases de datos, cumplimiento de estándares de seguridad, entre otros temas relativos a la protección de datos personales y la materia de esta ley, tanto a entes del sector público como el privado, para lo cual quedará habilitada a la venta de servicios, cuyo costo se establecerá mediante un tarifario de publicación y actualización periódica. Los precios de dicho tarifario deberán demostradamente estar acordes con los valores del mercado.

En el ejercicio de sus atribuciones, la Prodhab podrá emplear procedimientos automatizados, de acuerdo con las mejores herramientas tecnológicas a su alcance.

ARTÍCULO 39.- Dirección de la Agencia

La Dirección de la Prodhab estará a cargo de un director o una directora nacional, quien deberá contar, al menos, con el grado académico de licenciatura en una materia afín al objeto de su función, ser de reconocida solvencia profesional y moral, y tener comprobada experiencia y conocimiento en la materia de protección de datos personales.

El término de su nombramiento será por un período de hasta 4 años. En caso de declararse la vacancia, según lo dispuesto en este capítulo, la designación de la persona sustituta no podrá hacerse por un término mayor al que faltare para completar el período respectivo. Podrá ser reelecta por una única ocasión de forma continua.

No podrá ser nombrado director o directora nacional ninguna persona que sea propietaria, accionista, miembro de la junta directiva, gerente, asesora, representante legal o empleada de una empresa dedicada a la recolección, el almacenamiento y/o procesamiento de datos personales. Dicha prohibición persistirá hasta por dos años después de haber cesado sus funciones o vínculo empresarial. Estará igualmente impedido quien sea cónyuge o pariente hasta el tercer grado de consanguinidad o afinidad de una persona que esté en alguno de los supuestos mencionados anteriormente.

ARTÍCULO 40.- Proceso de nombramiento de la Dirección

La persona directora será nombrada por la Asamblea Legislativa. Para dicho nombramiento, la Asamblea anunciará el concurso de forma pública y podrá recibir postulaciones de cualquier persona que cumpla con los requisitos establecidos en esta Ley. La Comisión de Nombramientos definirá un procedimiento para estudiar dichas postulaciones, el cual deberá garantizar el cumplimiento de dichos requisitos, además de determinar mediante calificaciones objetivas la idoneidad y conocimiento de las diferentes personas candidatas. Al concluir dicho procedimiento, recomendará una terna de personas postulantes al Plenario.

El Plenario Legislativa elegirá, mediante votación pública y con mayoría absoluta, a la persona que dirigirá a la Prodhab. El Plenario podrá no apegarse a la recomendación emitida por la Comisión solamente de entre las personas postulantes.

ARTICULO 41.- Juramentación. La persona directora de la Prodhab debe rendir el juramento previsto en el artículo 194 de la Constitución Política ante el Plenario de la Asamblea antes de iniciar sus labores en el cargo.

ARTICULO 42.- Causas de cesación. La persona directora de la Prodhab de la República cesará en sus funciones, por cualquiera de las siguientes causales:

a) Renuncia a su cargo.

b) Muerte o incapacidad sobreviniente

c) Negligencia notoria o por violaciones graves al ordenamiento jurídico en el cumplimiento de los deberes de su cargo

d) Incurrimiento en cualquiera de las incompatibilidades previstas en esta Ley

e) Haber sido condenado, en sentencia firme, por delito cometido en forma dolosa.

La Asamblea Legislativa debe declarar vacante el cargo de la Dirección Nacional de la Prodhab, cuando se presente una de las causales previstas en los incisos a), b), d) y e) del presente artículo.

En el caso del inciso c), la Presidencia Legislativa nombrará una Comisión que le dará audiencia a la persona directora e informará a la Asamblea Legislativa, el resultado de la investigación, en el término de quince días hábiles.

ARTÍCULO 43.- Dirección Adjunta

La Asamblea Legislativa nombrará una persona como Director o Directora Adjunta, de una lista de tres candidatos propuestos por la persona Directora Nacional, a más tardar un mes después de su nombramiento. Quien ocupe la Dirección Adjunta deberá reunir los mismos requisitos exigidos para el cargo titular y estará sometido a las mismas prohibiciones y disposiciones que esta ley impone a ese cargo.

La personas elegida en este cargo será colaborador directo del Director Nacional de la PRODHAB; cumplirá las funciones que éste le asigne y lo sustituirá en sus ausencias temporales.

ARTÍCULO 44.- Personal de la Agencia

La Prodhab contará con el personal técnico y administrativo necesario para el buen ejercicio de sus funciones, designado mediante concurso por idoneidad, según el Estatuto de Servicio Civil o bien como se disponga reglamentariamente. El personal está obligado a guardar secreto profesional y deber de confidencialidad de los datos de carácter personal que conozca en el ejercicio de sus funciones.

ARTÍCULO 45.- Prohibiciones para las personas funcionarias

Todas las personas funcionarias de la Prodhab tendrán las siguientes prohibiciones:

a) Prestar servicios a las personas o empresas que se dediquen al acopio, el almacenamiento, o el manejo de datos personales. Dicha prohibición persistirá hasta dos años después de haber cesado sus funciones.

b) Involucrarse, personal e indebidamente, en asuntos conocidos en el marco de las funciones de la Agencia.

c) Revelar o de cualquier forma propalar los datos personales a que ha tenido acceso con ocasión de su cargo. Esta prohibición persistirá indefinidamente aun después de haber cesado en su cargo.

d) En el caso de los funcionarios y las funcionarias nombrados en plazas de profesional, ejercer externamente su profesión. Lo anterior tiene como excepción el ejercicio de la actividad docente en centros de educación superior o la práctica liberal a favor de parientes por consanguinidad o afinidad hasta el tercer grado, siempre que no se esté ante el supuesto del inciso a).

La inobservancia de cualquiera de las anteriores prohibiciones será considerada falta gravísima, para efectos de aplicación del régimen disciplinario, sin perjuicio de las otras formas de responsabilidad que tales conductas pudieran acarrear.

ARTÍCULO 46.- Presupuesto

El presupuesto de la Prodhab estará constituido por lo siguiente:

a) Los cánones, las tasas y los derechos obtenidos en el ejercicio de sus funciones.

b) Las transferencias que el Estado realice a favor de la Agencia.

c) Las donaciones y subvenciones provenientes de otros Estados, instituciones públicas nacionales u organismos internacionales, siempre que no comprometan la independencia, transparencia y autonomía de la Agencia.

d) Lo generado por sus recursos financieros.

e) Lo generado por la venta de servicios de asesoría, capacitación técnica y certificaciones en materia de privacidad, manejo de bases de datos, cumplimiento de estándares de seguridad, entre otros temas relativos a la protección de datos personales y la materia de esta ley.

Los montos provenientes del cobro de las multas señaladas en esta ley serán destinados a gastos de capital de la Prodhab.

La Agencia estará sujeta al cumplimiento de los principios y al régimen de responsabilidad establecidos en los títulos II y X de la Ley N.° 8131, Administración Financiera de la República y Presupuestos Públicos, de 18 de septiembre de 2001. Además, deberá proporcionar la información requerida por el Ministerio de Hacienda para sus estudios. En lo demás, se exceptúa a la Agencia de los alcances y la aplicación de esa ley. En la fiscalización, la Agencia estará sujeta, únicamente, a las disposiciones de la Contraloría General de la República.

SECCIÓN II

REGISTRO DE ARCHIVOS Y BASES DE DATOS

ARTÍCULO 47.- Registro de archivos y bases de datos

Toda base de datos, pública o privada, debe inscribirse en el registro que al efecto habilite la Prodhab, exceptuando aquellas sin fines comerciales administradas por personas físicas. La inscripción no implica el traspaso o la transferencia de los datos.

La Prodhab definirá, al momento del registro y de acuerdo a la envergadura, características y riesgos del tratamiento de datos que se realizará, si la persona responsable de la base de datos deberá cumplir, y en qué medida, con lo dispuesto en el capítulo II, Sección IV de esta Ley, respecto a Estudios de impacto, Protocolo de Actuación y la Persona Delegada de protección de datos. Los criterios y plazos para dicho cumplimiento se establecerán en lineamientos que al respecto confeccionará y revisará periódicamente la Prodhab.

CAPÍTULO V

PROCEDIMIENTOS

SECCIÓN I

NORMAS DE PROCEDIMIENTO

ARTÍCULO 48.- Legitimación para denunciar

Cualquier persona, grupo de personas u organismos debidamente habilitados para representar personas que ostente un derecho subjetivo o un interés legítimo puede denunciar, ante la Prodhab, que una base de datos pública o privada se encuentra en contravención de las reglas o los principios básicos para la protección de los datos y la autodeterminación informativa establecidas en esta ley.

ARTÍCULO 49.- Trámite de las denuncias

Todo procedimiento ordinario se regirá por el Libro Segundo de la Ley General de la Administración Pública, sin perjuicio de las regulaciones específicas que se puedan establecer vía el reglamento.

En cualquier momento, la Prodhab podrá ordenar a la persona denunciada la presentación de la información necesaria. Asimismo, podrá efectuar inspecciones in situ en sus archivos o bases de datos. Para salvaguardar los derechos de la persona o del grupo de personas interesadas, puede dictar, mediante acto fundado, las medidas cautelares que aseguren el efectivo resultado del procedimiento.

ARTÍCULO 50.- Efectos de la resolución estimatoria

Si se determina que la información del interesado es falsa, incompleta, inexacta, o bien, que de acuerdo con las normas sobre protección de datos personales esta fue indebidamente recolectada, almacenada o difundida, deberá ordenarse su inmediata supresión, rectificación, adición o aclaración, o bien, impedimento respecto de su transferencia o difusión. Si la persona denunciada no cumple íntegramente lo ordenado, estará sujeta a las sanciones previstas en esta y otras leyes.

SECCIÓN II

RÉGIMEN SANCIONATORIO

ARTÍCULO 51.- Procedimiento sancionatorio

De oficio o a instancia de parte, la Prodhab podrá iniciar un procedimiento tendiente a demostrar si un tratamiento de datos personales regulado por esta ley está siendo empleado de conformidad con sus principios; para ello, deberán seguirse los trámites previstos en la Ley General de la Administración Pública para el procedimiento ordinario.

ARTÍCULO 52.- Faltas leves

Las faltas leves, señaladas en este artículo, se sancionarán con multas administrativas de hasta de diez salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República como máximo o, si se trata de una empresa, con una multa equivalente al 2% del volumen de negocio total anual global del ejercicio financiero anterior como máximo, optándose por la multa de mayor cuantía.

Serán consideradas faltas leves, para los efectos de esta ley:

a) Recolectar datos personales para su uso en base de datos sin que se le otorgue suficiente y amplia información a la persona interesada, de conformidad con las especificaciones indicadas en esta ley.

b) Recolectar, almacenar y transmitir datos personales de terceros por medio de mecanismos inseguros o que de alguna forma no garanticen la seguridad e inalterabilidad de los datos.

.

ARTÍCULO 53.- Faltas graves

Las faltas graves, señaladas en este artículo, se sancionarán con multas administrativas de entre diez y cuarenta salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República o, si se trata de una empresa, con una multa equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior como máximo, optándose por la multa de mayor cuantía.

Serán consideradas faltas graves, para los efectos de esta ley:

a) Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento informado y expreso del titular de los datos, con arreglo a las disposiciones de esta ley.
b) Transferir datos personales a otras personas o empresas en contravención de las reglas establecidas en el capítulo III de esta ley.
c) Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información.
d) Negarse injustificadamente a dar acceso a un interesado sobre los datos que consten en archivos y bases de datos, a fin de verificar su calidad, recolección, almacenamiento y uso conforme a esta ley.
e) Negarse injustificadamente a eliminar o rectificar los datos de una persona que así lo haya solicitado por medio claro e inequívoco.

Artículo 54. - Faltas gravísimas

Las faltas gravísimas, señaladas en este artículo, se sancionarán con multas administrativas de entre treinta y sesenta salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República o, si se trata de una empresa, con una multa equivalente al 6% del volumen de negocio total anual global del ejercicio financiero anterior como máximo, optándose por la multa de mayor cuantía.

Serán consideradas faltas gravísimas, para los efectos de esta ley:

a) Recolectar, almacenar, transmitir o de cualquier otra forma emplear, por parte de personas físicas o jurídicas privadas, datos sensibles, según la definición prevista en el artículo 3 de esta ley.

b) Obtener, de los titulares o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza.

c) Revelar información registrada en una base de datos personales cuyo secreto esté obligado a guardar conforme la ley.

d) Proporcionar a un tercero información falsa o distinta contenida en un archivo de datos, con conocimiento de ello.

e) Realizar tratamiento de datos personales sin encontrarse debidamente inscrito ante la Prodhab, en el caso de los responsables de bases de datos cubiertos por el artículo 21 de esta ley.

f) Transferir, a las bases de datos de terceros países, información de carácter personal de los costarricenses o de los extranjeros radicados en el país, sin el consentimiento de sus titulares.

Artículo 55.- Criterios para establecer la sanción

Para tomar una determinación sancionatoria, el tipo de sanción y su cuantía, la Prodhab deberá considerar los siguientes criterios, sin perjuicio de valorar las infracciones de manera acumulativa:

a. **Naturaleza de la infracción:** número de personas afectadas, daños sufridos, duración de la infracción y propósito del procesamiento, infracción leve, grave o gravísima.

b. **Intención:** si la infracción es intencional o debido a negligencia

c. **Mitigación:** acciones tomadas para mitigar el daño a las personas interesadas

d. **Medidas preventivas:** cuánta preparación técnica y organizativa había implementado previamente la empresa para evitar el incumplimiento

e. **Reincidencia:** Posibles infracciones anteriores, incluido advertencias y multas relacionadas a similares u otras infracciones en área de seguridad digital, privacidad y protección de datos.

f. **Cooperación:** cuán cooperativa ha sido la empresa con la autoridad supervisora para remediar la infracción.

g. **Tipo de datos afectados:** qué tipos de datos impactado por la infracción.

h. **Notificación:** si la infracción fue notificada proactivamente a la autoridad supervisora por la propia empresa o un tercero.

SECCIÓN III

PROCEDIMIENTOS INTERNOS

ARTÍCULO 56.- Régimen sancionatorio para bases de datos públicas

Cuando la persona responsable de una base de datos pública cometa alguna de las faltas anteriores, la Prodhab dictará una resolución estableciendo las medidas que proceda adoptar para que cesen o se corrijan los efectos de la falta. Esta resolución se notificará a la persona responsable de la base de datos, al órgano del que dependa jerárquicamente y a los afectados, si los hay. La resolución podrá dictarse de oficio o a petición de parte. Lo anterior sin perjuicio de la responsabilidad penal en que haya incurrido.

CAPÍTULO VI

CÁNONES

ARTÍCULO 57.- Canon por regulación y administración de bases de datos

Las bases de datos que deban inscribirse ante la Prodhab, de conformidad con el artículo 41 de esta ley, estarán sujetas a un canon de regulación y administración de bases de datos que deberá ser cancelado anualmente, con un monto de trescientos dólares ($300), moneda de curso legal de los Estados Unidos de América, canon que se actualizará anualmente con base en el índice de valuación determinado por el comportamiento de la tasa de inflación (índice de precios al consumidor que calcula la Dirección General de Estadística y Censos).

Podrán eximirse del pago de este canon aquellas bases de datos utilizadas a lo interno de empresas o instituciones públicas, cuando sean utilizadas con fines

exclusivamente administrativos y sin fines de comercialización, y así se demuestre ante la Prodhab.

También podrán eximirse de dicho pago las bases de datos utilizadas por organizaciones sin fines de lucro (como fundaciones, sindicatos, asociaciones, organizaciones religiosas, entre otras), cuando demuestren que la finalidad de la base no es de ninguna índole comercial o de lucro.

La exención de este pago no les excluye del cumplimiento de esta ley en todos sus alcances, incluidos los pagos producto de infracciones a la Ley. Quedan a salvo aquellas excepciones que se puedan aplicar puntualmente. El procedimiento para realizar el cobro del presente canon será detallado en el reglamento que a los efectos deberá emitir la Prodhab.

ARTÍCULO 58.- Canon por comercialización de consulta

La persona responsable de la base de datos deberá cancelar a la Prodhab un canon por cada venta de los datos de ficheros definidos en el inciso l) del artículo 4 de esta ley, de personas individualizables registradas legítimamente y siempre que sea comercializado con fines de lucro, el cual oscilará entre los veinticinco centavos de dólar ($0,25) y un dólar ($1), moneda de curso legal de los Estados Unidos de América, monto que podrá ser fijado dentro de dicho rango vía reglamento. En caso de contratos globales de bajo, medio y alto consumo de consultas, o modalidades contractuales de servicio en línea por número de aplicaciones, será el reglamento de la ley el que fije el detalle del cobro del canon que no podrá ser superior al diez por ciento (10%) del precio contractual.

CAPÍTULO VI

TRANSFERENCIA TRANSFRONTERIZA DE DATOS PERSONALES

SECCIÓN ÚNICA

DE LAS TRANSFERENCIAS

ARTÍCULO 59.- Principio general de las transferencias

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, a reserva de las demás disposiciones de la presente Ley, el responsable y el encargado del tratamiento cumplen las condiciones establecidas

en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

ARTÍCULO 60.- Transferencias basadas en un procedimiento de adecuación

Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la PRODHAB, haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

Al evaluar la adecuación del nivel de protección, la PRODHAB tendrá en cuenta, en particular, los siguientes elementos:

a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; y,
b) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros,

ARTÍCULO 61.- Transferencias mediante garantías adecuadas

A falta de una autorización de la PRODHAB, por vía de un Procedimiento de Adecuación, el responsable o el encargado del tratamiento sólo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido

garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Las garantías adecuadas podrán ser aportadas, por:

a) Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) Convenios empresariales suscritos que expresamente reconozcan todos los derechos y obligaciones establecidos en la presente Ley, y se sujeten a la competencia de la Agencia de Protección de Datos de los Habitantes, para la debida protección de los datos personales en todos los alcances previstos por la presente normativa, respecto del tratamiento realizado fuera del ámbito de competencia territorial.

Esta norma aplicará en igual sentido, bajo el concepto de Grupo de Interés Económico, en los términos que establece la presente Ley.

ARTÍCULO 62.- Excepciones para situaciones específicas

En ausencia de una autorización producto de un Procedimiento de Adecuación o de Garantías Adecuadas, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) El interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) La transferencia sea necesaria por razones de interés público comprobado consistentemente;

e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento”

TRANSITORIOS

TRANSITORIO I.-

Las personas físicas o jurídicas, públicas o privadas, propietarias o administradoras de las bases de datos objeto de esta ley, deberán adecuar sus procedimientos, protocolos, contenidos de bases de datos y reglas de actuación a lo estipulado en la presente reforma, en un plazo máximo de un año.

TRANSITORIO II.-

El Poder Ejecutivo adecuará el reglamento a la Ley Nº 8968 previamente existente de acuerdo a los lineamientos establecidos en la presente reforma, en un plazo máximo de seis meses después de su entrada en vigencia, recogiendo las recomendaciones técnicas y legales que la Prodhab le proporcione.

TRANSITORIO III.-

Por un período de 8 años a partir de la entrada en vigencia de esta Ley, la Asamblea Legislativa dispondrá que se otorgue al menos un 5% de crecimiento anual a las transferencias que realiza el Estado a la Agencia, con el objetivo de fortalecer su labor de fiscalización, de realización de auditorías de oficio y de cobro de multas por infracciones a Ley Nº 8968.

Rige a partir de su publicación.

ENRIQUE SÁNCHEZ CARBALLO Y OTROS(AS) DIPUTADOS(OS)

El expediente legislativo aún no tiene Comisión asignada